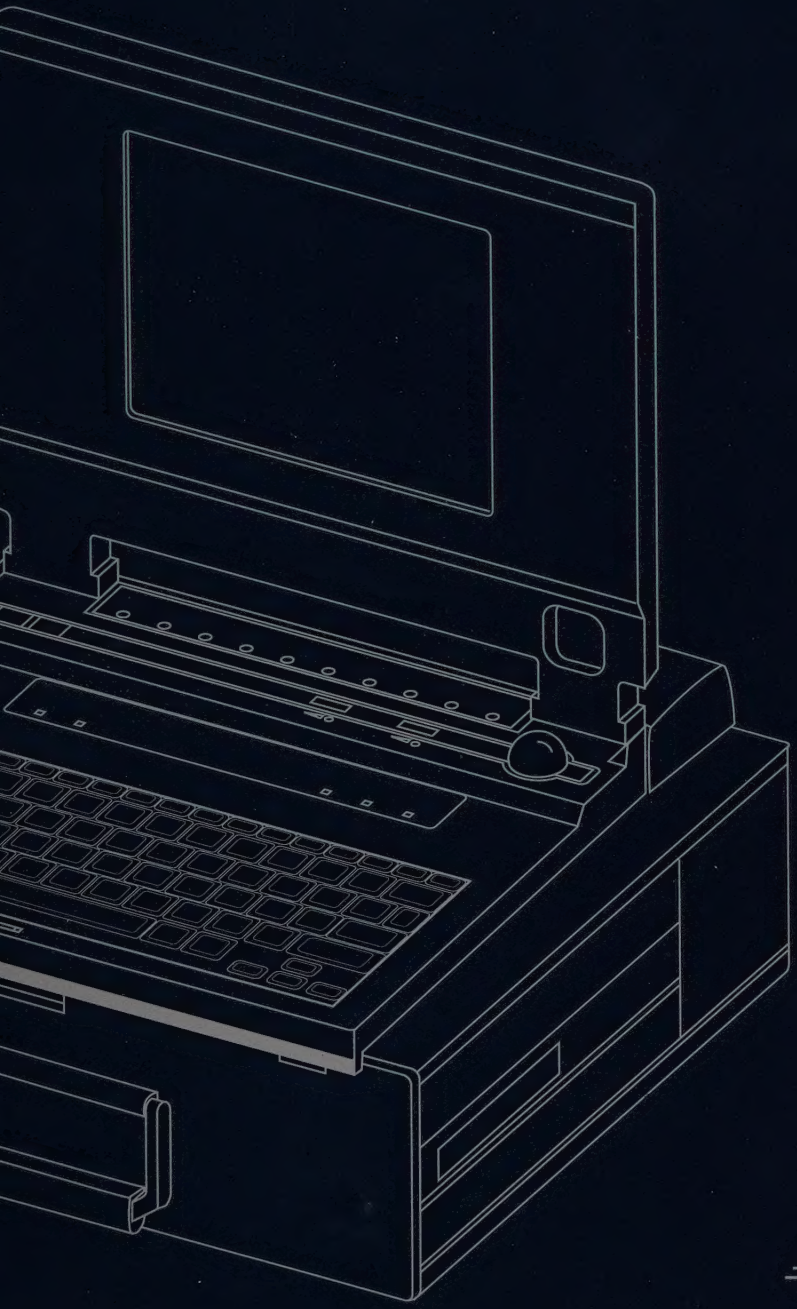
FIREBERD® 300/500



LAN Analyzer User's Guide

TTC™
A Dynatech Company

50-14039-01

FIREBERD 300/500
LAN ANALYZER

USER'S GUIDE

DECEMBER 1994

Rev. A

©1994 Telecommunications Techniques Corporation®
20400 Observation Drive, Germantown, Maryland 20876
Tel. (800) 638-2049 • (301) 353-1550 • FAX (301) 353-9216
WWW Address: http://www.ttc.com

Specifications, terms, and conditions are subject to change without notice.

TABLE OF CONTENTS

SECTION		PAGE
1.0	**LAN ANALYZER OVERVIEW**	**1-1**
1.1	Section Summary	1-1
1.2	What the LAN Analyzer Does	1-1
1.3	Concepts Behind the LAN Analyzer	1-1
1.4	Top Level Menus	1-2
1.5	The Tasks	1-3
1.6	Graphing, Logging, and Telnet	1-7
2.0	**INSTALLING AND CONNECTING THE LAN ANALYZER**	**2-1**
2.1	Section Summary	2-1
2.2	Installation Procedures	2-1
2.2.1	Check the Windows Setup	2-1
2.2.2	Installing the LAN Analyzer Module	2-2
2.2.3	Installing the LAN Software	2-2
2.2.4	Configuring PC/TCP	2-6
2.2.5	Testing the PC/TCP Software	2-8
2.3	Using the ADMIN Program	2-9
2.3.1	Selecting the Network Interface With the ADMIN Program	2-10
2.3.2	Exiting the ADMIN Program	2-12
2.4	Connecting the Analyzer to the Network	2-12
2.4.1	Connecting to Ethernet	2-13
2.4.2	Connecting to Token Ring	2-14
2.5	The EISA Configuration Utility	2-15
3.0	**USING THE LAN ANALYZER**	**3-1**
3.1	Section Summary	3-1
3.2	Starting the LAN Analyzer	3-1
3.3	Using the Analyzer Menu Functions	3-1
3.3.1	Adding of eleting an Analyzer Card (Only for FIREBERD 500)	3-2
3.3.2	Describing an Analyzer	3-2
3.3.3	Configuring an Analyzer	3-3
3.3.4	Selecting an Analyzer (Only for FIREBERD 500)	3-6
3.4	Ending the LAN Analyzer Session	3-6
3.4.1	Loading Saving and Deleting a Test	3-6
3.4.2	Ending the Session	3-7
3.4.3	Closing Down the LAN Analyzer	3-7

4.0 THE ANALYZER'S TASKS 4-1
4.1 Section Summary 4-1
4.2 Accessing the Tasks 4-1
4.3 Using the Host Stats 4-1
4.3.1 Setting up a Host Stats View 4-2
4.3.2 Cumulative Variables 4-3
4.3.3 Rate Variables 4-4
4.3.4 Percentage Variables 4-4
4.4 Using Segment Stats 4-5
4.4.1 Setting up a Segment Stats View 4-5
4.4.2 Cumulative Variables 4-6
4.4.3 Rate Variables 4-9
4.4.4 Percentage Variables 4-10
4.5 Using the Alarms 4-11
4.5.1 The Difference Between Alarms and Events 4-12
4.5.2 Alarms View Setup 4-12
4.5.3 Setting Up An Alarm 4-14
4.6 Using Matrix Stats 4-20
4.6.1 Setting up a Matrix Stats View 4-20
4.6.2 Changing the View 4-22
4.7 Using Packet Capture 4-23
4.7.1 Filters and Triggers 4-23
4.7.2 Setting Up Views to Capture Packets 4-23
4.7.3 Setting Up Capture 4-24
4.7.4 Setting Up Filters for Ethernet 4-25
4.7.5 Setting Up Filters for Token Ring 4-26
4.7.6 The TCP Filter Template - An Example 4-28
4.7.7 Destination, Source, Type, Data, and Invert Fields 4-33
4.7.8 Combining Filters 4-34
4.7.9 Using Triggers - An Example 4-36
4.7.10 Using a Trigger to Count Packets 4-37
4.7.11 Starting and Stopping Capture 4-38
4.7.12 Capture Slice Size 4-39
4.7.13 Capture Buffer Matches 4-39
4.7.14 Saving Capture Configurations 4-39
4.7.15 Displaying Packets 4-42
4.7.16 The Capture Display 4-42
4.8 Using Segment History 4-43
4.8.1 Setting Up a Segment History View 4-43
4.8.2 Creating and Deleting a Segment History Display 4-44
4.8.3 Available Segment History Statistics 4-45
4.9 Using Traffic Generation 4-48
4.9.1 Configuring Generation 4-48
4.9.2 The MAC Level Dialog for Ethernet 4-50

4.9.3 The MAC and LLC Level Dialog for Token Ring 4-52
4.9.4 Template Filters 4-53
4.9.5 Displaying Traffic Generation 4-54
4.9.6 General Traffic Generation Stoppage 4-55
4.9.7 Ethernet Traffic Generation Stoppage 4-56
4.9.8 Token Ring Traffic Generation Stoppage 4-56
4.10 Using the Test Application 4-56
4.10.1 Setting Up the Test Application 4-57
4.11 Using Ring Stats 4-59
4.11.1 Setting Up a Ring Stats View 4-60
4.11.2 Ring Stats Cumulative Variables 4-61
4.12 Using the Error 4-62
4.12.1 Setting Up an Error View 4-62
4.13 Using Protocol Stats 4-64
4.13.1 Setting Up a Protocol Stats View 4-64
4.13.2 Available Protocol Statistics 4-65
4.14 Displaying and Printing Information 4-65
4.14.1 Displaying Results as Tables 4-66
4.14.2 Displaying Results as Histograms 4-66
4.14.3 Saving and Printing Data 4-67

5.0 EVENTS, CUSTOM GRAPHING, AND LOGGING 5-1
5.1 Section Summary 5-1
5.2 Events and the Event Browser 5-1
5.2.1 Event Priority and Parameters 5-1
5.2.2 Acknowledging Events 5-2
5.2.3 Event Types 5-2
5.2.4 The Event Browser 5-3
5.2.5 Event Browser Options 5-4
5.2.6 Thresholds 5-5
5.2.7 The Event Log 5-5
5.3 Using the Graph Data Task 5-5
5.3.1 Setting Graph Parameters 5-6
5.3.2 Running Multiple Graphs 5-7
5.3.3 Ethernet Graphable Variables 5-7
5.3.4 Token Ring Graphable Variables 5-10
5.3.5 The Graph Display 5-14
5.3.6 Graph Options 5-14
5.4 Using the Log Data Task 5-16
5.4.1 Setting Logging Parameters 5-16
5.4.2 The Log Display 5-18
5.4.3 Logging Options 5-18
5.5 The Address Translation Table 5-19
5.6 TELNET 5-21

APPENDIX A PC/TCP SOFTWARE A-1
A.1 Introduction A-1
A.2 Command Description A-1
A.2.1 Ping A-1
A.2.2 Ping Options A-2
A.2.3 Error Messages from Ping A-4
A.2.4 Using Ping To Isolate Network Trouble A-5
A.2.5 Host A-5
A.2.6 Inet A-6
A.2.7 Inet Options A-7
A.3 Troubleshooting A-9
A.3.1 Error Messages A-9
A.3.2 Problems A-10
A.3.3 Responses From The Wrong Host A-10
A.3.4 No Response A-10
A.3.5 Responses From Local Hosts, But Not From Another Network A-10
A.4 Technical Notes A-11
A.4.1 Ethernet Analyzer Module Defaults A-11
A.4.2 Token Ring Analyzer Module Defaults A-12
A.4.3 PC/TCP Packet Driver Buffers A-13
A.4.4 PC/TCP Interaction with the LAN Analyzer Module A-13
A.14.5 PC/TCP Protocols A-13
A.4.6 IP A-14
A.4.7 UDP A-14
A.4.8 TCP A-14
A.5 Host Names and Internet Addresses A-14
A.5.1 Hostname Resolution A-15
A.5.2 Host Table Considerations A-16
A.5.3 Host Table Format A-16
A.5.4 Internet Addresses and Subnets A-17
A.5.5 Subnets A-17

FIGURES

1-1 LAN Analyzer Main Window 1-2
2-1 LAN Analyzer Setup Dialog Box 2-4
3-1 Describe Analyzer Box 3-2
3-2 The Configuration Box 3-4
3-3 The Apply Box 3-5
4-1 Host Statistics View Setup 4-2
4-2 Segment Statistics Setup 4-5
4-3 Alarms View Setup 4-12
4-4 Alarms View 4-13

4-5 Existing Alarms Window 4-14
4-6 Alarm Setup 4-15
4-7 Example Setup for a Per-Station Alarm 4-16
4-8 Select Stations 4-18
4-9 Matrix Statistics Select View Type 4-20
4-10 Matrix Stats Display 4-21
4-11 Matrix Stats Packet Data 4-22
4-12 Capture 4-24
4-13 Capture Setup 4-24
4-14 MAC Level Template 4-25
4-15 MAC and LLC Level Template 4-27
4-16 TCP Filter Template 4-28
4-17 Combining Filters 4-35
4-18 Example Using Triggers 4-36
4-19 Trigger Information 4-37
4-20 Capture Box Display 4-38
4-21 Setting Up Packet Display 4-40
4-22 Load File Box 4-41
4-23 Decoded Packet Display 4-42
4-24 Segment History View Setup 4-43
4-25 Traffic Generation Config 4-48
4-26 Bit Level Edit Box 4-50
4-27 Ethernet MAC Level Template 4-50
4-28 MAC and LLC Level Template 4-52
4-29 TCP Filter Template 4-53
4-30 Ethernet Traffic Generation Display 4-54
4-31 Token Ring Traffic Generation Display 4-55
4-32 Test Mode Configuration Box 4-57
4-33 Select Stations 4-58
4-34 Test Results in New View Window 4-59
4-35 Ring Station Statistics View Setup 4-60
4-36 Config Error 4-62
4-37 New View 4-63
4-38 Protocol Statistics View Setup Window 4-64
4-39 Example of a Table Display 4-66
4-40 Example of a Histogram Display 4-66
5-1 Event Browser Display 5-3
5-2 Graph Parameters Dialog Box 5-6
5-3 Graph Display 5-14
5-4 Setting Log Parameters 5-16
5-5 Specifying Threshold Values 5-17
5-6 Log Application Window 5-18
5-7 Address Translation Table 5-20
5-8 Telnet Window 5-21

TABLES

1-1 LAN Analyzer Top-level Menus 1-3
1-2 LAN Analyzer Task Summary 1-4
1-3 Graphing and Logging Task Summary 1-7
2-1 Basic ADMIN Commands 2-10

SECTION 1
LAN ANALYZER OVERVIEW

1.1 SECTION SUMMARY

This section gives you a high-level overview of the 300/500 Local Area Network Analyzer Modules. Described here are what the analyzers do, how they work, their top-level menus, and an introduction to the Analyzer's Tasks. For information specific to the FIREBERD 300/500 mainframe, refer to the *FIREBERD 300/500 Internetwork Analyzer User's Guide.*

1.2 WHAT THE LAN ANALYZER DOES

The FIREBERD 581 Ethernet LAN Analyzer, and FIREBERD 583 Token Ring LAN Analyzer are interface modules for the FIREBERD 500 Internetwork Analyzer mainframe. They enable the FIREBERD 500 to function as a portable LAN analyzer and Remote Network Monitoring (RMON)-based device for Ethernet and Token Ring networks.

Similarly, the FIREBERD 381 Ethernet LAN Analyzer, and FIREBERD 383 Token Ring LAN Analyzer are interface modules for the FIREBERD 300 Internetwork Analyzer mainframe. They enable the FIREBERD 300 to function as a portable LAN analyzer and Remote Network Monitoring (RMON)-based device for Ethernet and Token Ring networks.

The FIREBERD mainframe has been configured at the factory so you can begin capturing data from the network immediately, without a lengthy installation procedure. This User's Guide tells you how to configure the LAN Analyzer.

The LAN Analyzer's ability to take snapshots of segment performance, establish baseline criteria, filter and analyze packets, and decode protocols in plain English enables you to solve network problems easily.

The LAN Analyzer is scalable, too. Because its modular architecture supports multiple network topologies, you don't need to use another analyzer when the network changes.

1.3 CONCEPTS BEHIND THE LAN ANALYZER

This section introduces you to the main concepts behind the FIREBERD 500 LAN Analyzer. These concepts are protocol decodes, statistics, and events.

Protocol decodes

The heart of any analyzer is in its ability to decode protocols. The LAN Analyzer enables you to capture and decode most of the Ethernet and Token Ring protocols in use on the network. You can see these protocols displayed in plain English, so you can identify and solve problems quickly.

Statistics

Statistical data is information describing the operation of a device over a period of time. The LAN Analyzer enables you to identify the statistics that are important to you, and disregard the rest. Using the graphing and logging applications, you can set threshold values for statistics. You can graph statistics and log them to a file.

Events

Events show you when something significant happens on the network. When events occur, they cause the Event icon (a bell) to appear in the foreground of the screen. An event occurs when a threshold value is exceeded (this is a Rising Alarm), or when a level falls back below the threshold value (this is a Falling Alarm). The LAN Analyzer keeps a full record of events, and you can view the record using the Event Browser. You can also save events to a file.

The LAN Analyzer enables you to discard events that aren't critical to the test you are running, and keep the ones you wish to analyze. By saving specific events, you can conduct tests more quickly and efficiently than sorting through all the information that passed through the analyzer.

1.4 TOP LEVEL MENUS

This section introduces the functions of the LAN Analyzer's top-level menus. Figure 1-1 shows the LAN Analyzer's top-level menu choices.

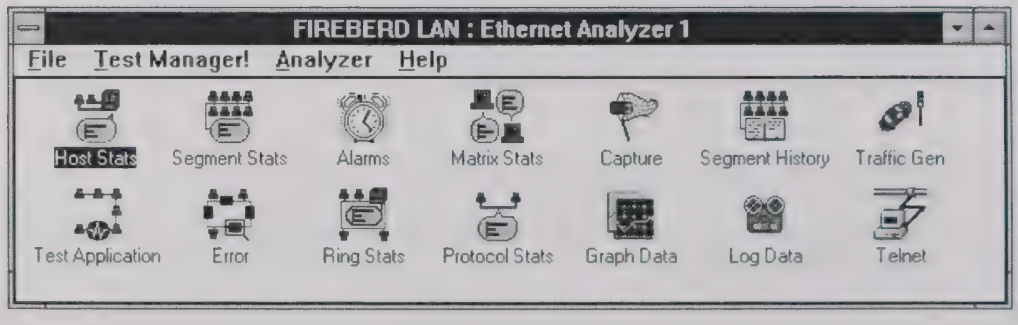


Figure 1-1
LAN Analyzer Main Window

Table 1-1 lists and briefly describes the top-level menus.

Table 1-1
LAN Analyzer Top-level Menus

Menu and Item:	What the Item Does:
File	
Load Session...	Opens a pre-configured session file.
Save Session...	Saves the session configuration to a file, and adds it to the directory.
Delete Session...	Deletes the session file from the directory.
Setup...	Displays the selected LAN Analyzer setup parameters.
Exit	Exits and shuts down the LAN Analyzer, and returns to the Test Manager.
Test Manager!	Returns you to the Test Manager with the LAN Analyzer still running.
Analyzer	
New...	Adds a new analyzer card or probe for use. (For FIREBERD 500 only)
Delete...	Removes an analyzer card. (For FIREBERD 500 only)
Describe...	Identifies and sets parameters for the analyzer card you selected.
Configure...	Changes configuration settings for the analyzer.
Select Analyzer...	Displays additional analyzers when there are more than 5 analyzer entries. (For FIREBERD 500 only)
Help	
General Index	Displays the table of contents for Help topics.
Applications	Shows the table of contents for topics within the LAN Tasks.
About...	Provides the version number of the LAN Analyzer software.

1.5 THE TASKS

The key to operating the LAN Analyzer is its eleven Tasks. Each one enables you to perform a specific activity that you'll be involved with during LAN testing. Icons on the top-level menu represent each Task; double-click on the icons in the top-level menu to access them.

Table 1-2 lists these Tasks, briefly describes the activity each one controls, and lists the section in this User's Guide where you can learn more about using the task to conduct the test.

Table 1-2
LAN Analyzer Task Summary

Task:	Lets You Do the Following:	To Learn More:
Host Stats	Collect and format statistics about the packets transmitted and received by the stations on the network.	See Section 4.3
Segment Stats	Collect and format statistics about network activity on a specified segment of the network. Display three types of statistics: Cumulative (counts of packets, bytes, or error packets), Rate (the number of packets of a given type per second sent by a host), and Percentage (the percentage of bandwidth used by packets to or from a host). Display up to 20 segment statistic sets simultaneously.	See Section 4.4
Alarms	Be notified when a specific event occurs, such as when a new station joins the network. Use the Events log to record the details of the event that triggered the alarm. Select the thresholds for segment activity specific to the network.	See Section 4.5
Matrix Stats	Examine the incoming and outgoing traffic on a selected station. Make lists of the addresses/names for all stations that send or receive traffic, along with the percentage of total traffic for each station.	See Section 4.6

Table 1-2
LAN Analyzer Task Summary (Continued)

Task:	Lets You Do the Following:	To Learn More:
Capture	Trigger on, filter, and capture packets from the network. Decode and display captured packets. Save captured packets to a file on the FIREBERD mainframe's hard drive.	See Section 4.7
Segment History	Take a snapshot of specified types of activity happening over a particular time interval on a selected segment of the network. Specify how many time intervals to select for each configuration of the Segment History.	See Section 4.8
Traffic Generation	Test how a network segment behaves under certain specified loads. Generate a packet from the contents of either a capture buffer or a template that you can define.	See Section 4.9
Test Application	Perform standard packet echo and forwarding tests on selected stations.	See Section 4.10
Ring Stats	Collect and display statistics about the packets transmitted and received by active hosts on a Token Ring network.	See Section 4.11
Error	Capture certain user-defined Media Access Control (MAC) error packets. Log and view cumulative statistical values calculated from the encountered error packets. Save the error events to a file as an ASCII copy of the viewed contents.	See Section 4.12

Table 1-2
LAN Analyzer Task Summary (Continued)

Task:	Lets You Do the Following:	To Learn More:
Protocol Stats	Collect and display statistics about packets transmitted and received using selected protocols. View several displays (such as several tables or histograms) simultaneously.	See Section 4.13
Displaying and Printing Information	View several displays (such as several tables or histograms) simultaneously.	See Section 4.14

1.6 GRAPHING, LOGGING, AND TELNET

The FIREBERD 300/500 LAN Analyzer has some extensive graphing and logging features. Additionally, the Telnet feature enables you to administer remote terminals. Table 1-3 lists these features, briefly describes the activity each one controls, and lists the section in this User's Guide where you can learn more about using them.

Table 1-3
Graphing and Logging Task Summary

Feature:	Lets You Do the Following:	To Learn More:
Events	Define what events are significant to the operation of the network. Know when something significant happens on the network.	See Section 5.2
Graph Data	Costomize graphs to show specific network objects and stastics. Establish and graph threshold values.	See Section 5.3
Log Data	Store parameter data over time in a file. Run up to five logs simultaneously from one task.	See Section 5.4
Address Translation Table	Identify stations by their MAC Address, name, segment, and IP Address. Define and name groups of stations in a table.	See Section 5.5
Telnet	Log in to a remote host. Remotely control and administer devices.	See Section 5.6

SECTION 2
INSTALLING AND CONNECTING THE LAN ANALYZER

2.1 SECTION SUMMARY

The LAN Analyzer software has been factory-installed if it was purchased with the FIREBERD 300/500 Internetwork Analyzer mainframe. However, if you purchased the LAN Analyzer separately, or need to re-install the software, this section shows you how to:

- install the LAN Analyzer software
- install the LAN Analyzer module into the FIREBERD 300/500 mainframe
- use the ADMIN program
- connect the LAN Analyzer to the network.

2.2 INSTALLATION PROCEDURES

This section provides installation procedures for the LAN Analyzer software and the LAN Analyzer module. If you have any questions on these procedures, call TTC's Applications Engineering Group at (800) 638-2049 or (301) 353-1550.

2.2.1 Check The Windows Setup

Windows 3.1 is factory-installed in the FIREBERD 300/500 mainframe. Using the Windows File Manager, open the `C:\CONFIG.SYS` file. This file should contain lines like these:

```
STACKS=9,256
FILES=50
BUFFERS=10,0
DEVICE=C:\DOS\HIMEM.SYS
```

NOTE: Be sure that you have 5 MB of hard disk space to complete the software installation. To check the disk space, at the C:\ prompt type `DIR`. The number listed as bytes free is the hard disk space available.

2.2.2 Installing the LAN Analyzer Module

Typically, the LAN Analyzer module has already been installed for you at the factory, but at some point you may want to re-install it. To install the Ethernet or Token Ring Analyzer module in any vacant slot in the FIREBERD 300/500 mainframe, perform the following steps:

1. Turn the power OFF before inserting or removing the LAN Analyzer module.

2. Insert the LAN Analyzer module into a vacant slot in the FIREBERD 300/500 mainframe.

3. Insert the flanges, located at the top of the LAN Analyzer module, into the slides located on the sides of the slot into which you're inserting the module.

4. Slowly slide the module into the mainframe, until it is properly seated in the mainframe mating connector. It will click into place.

   NOTE: When the module is properly installed, the small handles (located on either side of the module) are not sticking out but are parallel with the module front panel.

5. Connect the test cable to the LAN Analyzer connector for the circuit you are testing.

6. Turn the power ON.

7. If the test modules (in this case, the LAN Analyzer) installed in the mainframe are the same as when power was turned off, the Test Manager window is displayed.

If the mainframe configuration is not the same as when power was turned off, you will need to run the EISA configuration utility to reconfigure the mainframe resources. See Section 2.5, The EISA Configuration Utility, for the sequence of events that you will observe on the display if the mainframe configuration has changed.

2.2.3 Installing the LAN Software

The LAN Analyzer uses PC/TCP® software by FTP Software, Inc.® to enable the LAN Analyzer to function on a PC-based network. PC/TCP uses a Microsoft Windows type of installation procedure. Install and test the LAN software as described in the following steps.

First, check to see if the PC/TCP software has been installed on the FIREBERD 300/500. To check, follow these steps:

1. Shut off and reboot the FIREBERD 300/500.

2. As it is powering up, the following information about PC/TCP is displayed.

```
FTP Software PC/TCP Resident Module
PCTCP Virtual Device Version 3.0
Copyright (c) 1986 - 1994 by FTP software, Inc.  All Rights Reserved.
```

NOTE: If PC/TCP software is presently installed on the FIREBERD 300/500, you do not need to install it again.

To install the LAN software, perform the following steps:

1. Insert disk 1 labeled "FIREBERD LAN Software" into the FIREBERD 300/500 floppy drive. Start Windows, and with the Windows Program Manager displayed, pull down **File>Run**. Type: `A:SETUP`. The installation process automatically determines whether sufficient disk space is available; if there isn't enough space, a warning message appears and the installation stops. You will then have to free up more space to allow the installation to be completed.

2. The LAN Analyzer Setup message is displayed informing you that the mainframe is initializing the setup. Another message is displayed informing you that the installation will require about 5 M of disk space. Click on **Continue** to continue the software installation.

   NOTE: If the LAN software has already been installed, a message is displayed indicating that LAN software already has been installed. Press **Continue** to overwrite it (the existing software) with a new version or press **Exit** to cancel the installation.

3. Confirm the location of the AUTOEXEC.BAT file that is updated during the installation. Change this if you need to, then click on **Continue**.

4. A dialog box appears, asking you for the PC/TCP Serial Number (located on the disk). Enter this serial number and click on **Continue**. You are asked to confirm the serial number. After doing so, click on **Continue**.

   NOTE: If the Serial Numbers do not match, a message is displayed indicating such and returns you to the first Serial Number dialog box to reenter the valid number, followed by the confirmation dialog box.

5. The PC/TCP Authentication Key dialog box asks you to confirm the PC/TCP Authentication Key number (located on the disk). Enter the authentication key number and click on **Continue**. You are asked to confirm the authentication key number. After doing so, click on **Continue**. After installation of the PC/TCP software has been completed, the PC/TCP Setup Exit window tells you the installation was successful.

   NOTE: If the PC/TCP Authentication Key numbers do not match, a message is displayed indicating such and returns you to the Authentication Key dialog box to reenter the valid number, followed by the confirmation dialog box.

6. Follow the instructions displayed on the screen to insert the other LAN software disks.

7. When the LAN Analyzer Setup dialog box appears (as shown in Figure 2-1) enter, as a minimum, the following parameters:

   Setup
   Mode — None or Analyzer
   Router IP — Network dependent
   Local Host (i.e., the mainframe)
   IP Address — Network dependent
   Subnet Mask — Network dependent
   Analyzer (i.e., the LAN card)
   Card — Analyzer Card 1 (Ethernet) or Analyzer Card 2 (Token Ring)
   Media Type — Ethernet or **Ring Speed** — Token Ring
   IP Address — Network dependent
   Subnet Mask — Network dependent

   Then click on **OK**.

NOTE: The IP Addresses entered must be on the same subnetwork.

NOTE: If None is the Mode selection, all other parameters are grayed out or blank.

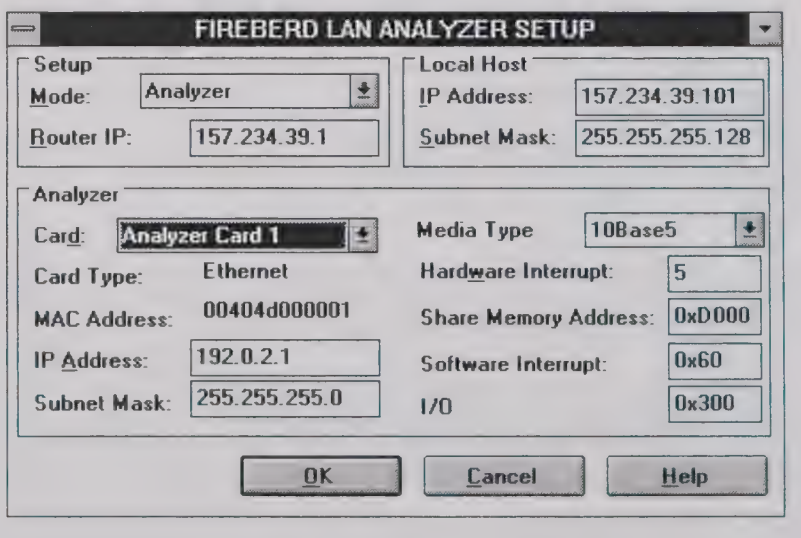


Figure 2-1
LAN Analyzer Setup Dialog Box

8. If all the information entered in the FIREBERD LAN Analyzer Setup dialog box is accepted, a message is displayed indicating that the FIREBERD LAN Analyzer has been successfully installed on the hard drive and requesting to reboot the PC before running the program.

9. Click on **OK**.

10. Reboot the PC.

NOTE: Making any change to information on the FIREBERD LAN Analyzer Setup dialog box requires the PC to be rebooted.

FIREBERD LAN Analyzer Setup dialog box parameter choices are listed and described in the following paragraphs.

Setup

Mode — Selects the LAN Analyzer operating mode. Choices are: None or Analyzer. Selecting None disables the LAN drivers and software. Analyzer gives the mainframe access to the LAN module.

Router IP — Enter the network router IP address for the local segment.

Local Host

IP Address — Enter the IP address for the FIREBERD mainframe. Network dependent.

Subnet Mask — Enter the subnet mask for the FIREBERD mainframe. Network dependent.

Analyzer

Card — Selects the type of LAN card that is active. Choices are: Analyzer Card 1 (Ethernet) or Analyzer Card 2 (Token Ring).

Card Type — Indicates the LAN card selection. This parameter is not selectable and indicates: Ethernet or Token Ring.

MAC Address — Indicates the MAC address for the selected LAN Analyzer card. Assigned by the manufacturer.

IP Address — Enter the IP address for the LAN Analyzer card. Network dependent.

Subnet Mask — Enter the subnet mask for the LAN Analyzer card. Network dependent.

Media Type — Select the media type when **Card** is set to Analyzer Card 1 (an Ethernet card). Media Type choices are: 10Base2, 10Base5, or 10BaseT.

Ring Speed	Select the ring speed when **Card** is set to Analyzer Card 2 (a Token Ring card). Ring Speed choices are: 4M Ring or 16M Ring. Failure to set the ring speed properly may cause beaconing and even segment failure.
Hardware Interrupt	Indicates the mainframe hardware interrupt initiated by the selected LAN card. LAN Analyzer card dependent.
Share Memory Address	Indicates the high memory address shared by the mainframe and the selected LAN card. Card dependent.
Software Interrupt	Indicates the software interrupt used the selected LAN card to access a driver. LAN Analyzer card dependent.
I/O	Indicates the I/O address used by the mainframe to communicate with the selected LAN card. LAN Analyzer card dependent.

NOTE: Any changes made in the FIREBERD LAN Analyzer Setup dialog box requires the mainframe to be rebooted before taking effect. Also keep in mind that software changes made to: Hardware Interrupt, Share Memory Address, Software Interrupt, and I/O must be made to hardware on the LAN card.

Assigning an IP Address and a Subnet Mask

Before using PC/TCP, you will need to enter some information about the network. As a minimum, an IP address and subnet mask must be assigned to the FIREBERD 300/500. You may also need to set up a default router and a name server. Contact the system administrator if this information is not available to you; if it is available to you, follow the directions in the following section.

2.2.4 Configuring PC/TCP

PC/TCP uses a Windows-like initialization file. This section describes how to change the configuration of PC/TCP.

Use a text editor (e.g., Windows Notepad or DOS Editor) to edit the PCTCP.INI file. This file is located in the path `C:\fb500\lan\PCTCP.INI` unless you specified a different directory when you installed the PC/TCP software. A sample file follows:

```
[pctcp kernel]
serial-number=1990-1111-2222
authentication-key=1234-5678-1234
interface=ifcust 0
host-table=c:\FB500\LAN\HOSTS
```

```
[pctcp general]
use-old-init-scheme=no
domain=
hostname=
etc-dir=c:\FB500\LAN

[pctcp ifcust 0]
ip-address=1.2.3.4
subnet-mask=255.255.0.0
router=

[pctcp addresses]
domain-name-server=
```

Note that the file has four sections: `pctcp kernel`, `pctcp general`, `pctcp ifcust 0`, and `pctcp addresses`. Each section contains one or more lines consisting of a parameter and a value. To change the settings of the PC/TCP software, edit and save the new settings in this file. Once you've made all of the changes, reboot the FIREBERD 300/500 so the changes can take effect. The following paragraphs describe each section in more detail.

pctcp kernel

The only parameter that you may need to change in `pctcp kernel` is host-table, which is used to specify the path to an IP address for the host-name look-up table. If you are not using a host table, leave the value for this parameter blank. For more information about host tables, see Appendix A, at the back of this manual.

pctcp general

`pctcp general` contains the parameters for the analyzer's domain name and host name. They are needed if you are using a domain-name server. For example, if the analyzer's fully-qualified domain name is `panther.tt.com`, then `tt.com` is the domain name and `panther` is the host name.

pctcp ifcust 0

The parameters for `pctcp if cust 0` describe the network interface in the FIREBERD 300/500.

NOTE: Before you can use the LAN Analyzer on a network, you must configure it with an IP address and a subnet mask. If this information is not available to you, consult the system administrator.

If the FIREBERD 300/500 needs to talk across LAN segments through a router, enter the default router IP address as the value for the router parameter. If you have multiple routers on the segment, list them on separate lines.

pctcp addresses

If you are using a domain name server for IP address resolution, the domain-name-server parameter should be set to the IP address of the name server. If you are using multiple servers, list them on separate lines. You will also need to set up a domain name and host name under the `pctcp general` section above.

2.2.5 Testing the PC/TCP Software

Reboot the FIREBERD 300/500 after changing the PC/TCP configuration file, so the new configuration can be loaded.

Before running the LAN Analyzer software, test the PC/TCP configuration to be sure it is correct and that the network card and connection are working. The best way to do this is to "ping" a host on the network.

Ping sends an echo request packet to a host and waits for a response. It reports success or failure and an array of statistics about its operation. Both a client and a server are provided, so echo requests can be sent from the LAN Analyzer, and it can reply to other hosts on the network.

For example, assume "wayward" is the name of a host on the network. Type the following at the `C:\` prompt:

```
ping wayward
```

Refer to Appendix A.5 for hostname resolution.

If the LAN Analyzer is configured and connected correctly, the response would be:

```
host responding, time = X ms
```

Here, *X* is the number of milliseconds it took the host to respond. If the PC/TCP software is not installed correctly, the most likely error messages would be:

`Network Unreachable`	If you get this response, be sure you set the IP address correctly.
`Ping failed: timeout`	If you get this response, be sure the host that you pinged is up, and check the cable connection to the FIREBERD 300/500.

Resolve any faults that may occur before proceeding.

2.3 USING THE ADMIN PROGRAM

The ADMIN program is a DOS-based group of commands that you use to set up the IP address and subnet mask, and to configure the LAN Analyzer for use on the network. Most of the changes you make using the ADMIN program don't take effect until you reboot the FIREBERD 300/500. To access the ADMIN program, do the following:

1. Close out of the LAN Analyzer, Test Manager, and Windows to get to the `c:\` prompt. Or, with the Windows Program Manager displayed on the screen, click on the MSDOS Prompt icon in the **Main** group.

2. At the `c:\` prompt, type `ADMIN` and press **<Enter>**. The screen should look like this:
   ```
   ADMIN.exe Analyzer Card Admin Program - (c) TTC, 1993-1994
   Examining system initialization file, please wait...
   ```

   Type the number of the analyzer card you wish to use. The number should correspond to the card numbers given in the `ANALYZER.INI` file.

3. Next, the screen should display:
   ```
   Opening Connection to Analyzer Card X (press F1 to exit):
   ```

   (X refers to the number of the analyzer card you're using.)

   Press **<Enter>** to start the ADMIN session, and the screen should display the following prompt:
   ```
   Ethernet>
   Token>
   ```

   You are now in an ADMIN session and ready to enter commands.

2.3.1 Selecting the Network Interface With the ADMIN Program

You can use the ADMIN program to select the network interface. Although there are several ADMIN commands, Table 2-1 lists the basic commands you will need. Pressing **<Ctrl + C>** will exit out of the command and cancel any changes you may have made.

Table 2-1
Basic ADMIN Commands

Command:	Abbr.:	Function:
HELP	**?**	Briefly describes the ADMIN commands available.
SETMEDIATYPE	**SMT**	Configure the Ethernet media type; for Ethernet modules only.
CHADDRESS	**CA**	Change address; change the IP addressing parameters.
SETRINGSPEED	**SRS**	Set Token Ring speed; for Token Ring modules only.
BOOT	**BO**	Reboot analyzer card.
QUIT	**Q**	Leave the ADMIN program.

HELP (?)

The **HELP** command displays a brief description of each command in the ADMIN program. To display the description for a certain command, type `help` and the abbreviation for that command. For example, if you wanted help on the **CHADDRESS** command, type `help ca` or `help chaddress`. The screen then displays:

```
CHADDRESS    (or CA) - change the IP addressing parameters
```

SETMEDIATYPE (SMT)

The **SETMEDIATYPE** command only applies to the Ethernet LAN Analyzer. **SETMEDIATYPE** configures the analyzer to use the type of physical media that you attach to it. The analyzer cannot operate on an Ethernet LAN until you set the media type.

When you enter **SETMEDIATYPE**, the analyzer displays these prompts:

```
Media Type <10Base5, 10BaseT, or 10Base2> ?
```

10Base2 is the default setting. Enter the media type you will be using on the network, and press **<ENTER>**.

CHADDRESS (CA)

The **CHADDRESS** command configures IP addressing information. The parameters are:

`Internet address` This is the Internet address for the Ethernet or Token Ring card. Enter any address in the form b1.b2.b3.b4 or NONE. The numbers b1 to b4 may be specified in decimal or hexadecimal (prefix each hexadecimal digit with "0x") formats.

`Subnet mask` Enter a subnet mask to subdivide a class A, B, or C network with routing done by gateways. Or, enter NONE to select one of the following defaults which are used according to the class of the IP address:

```
class A     255.0.0.0
class B     255.255.0.0
class C     255.255.255.0
```

SETRINGSPEED (SRS)

The **SETRINGSPEED** command only applies to the Token Ring LAN Analyzer. **SETRINGSPEED** lets you specify to the LAN Analyzer what Token Ring speed to use.

In response, the analyzer displays this prompt:

```
Ring Speed < 4 or 16 >?
```

Enter the correct speed for the network.

BOOT (BO)

The **BOOT** command reboots the analyzer card. If you choose to reboot, the following message appears:

```
Rebooting the analyzer will lose all network statistics
Do you wish to restart the analyzer?  <YES or NO> ?
```

QUIT (Q)

The **QUIT** command exits the ADMIN session. If you have changed the configuration, the following message is displayed while non-volatile memory is updated.

```
Checking nonvolatile memory.......
```

When the update is completed, the following message is displayed.

```
Parameter changes stored in nonvolatile memory.
```

The analyzer can be safely switched off after this message has been displayed. If the analyzer detects a change that will not take effect until the next software restart, the following message is displayed:

```
The analyzer should be restarted for all changes to take effect.
Do you wish to restart the analyzer [YES or NO]?
```

If you enter NO, N, **<Ctrl + C>**, or you allow the command to time out, the analyzer will not be restarted. Enter YES or Y to restart the analyzer software. In either case, the analyzer exits the ADMIN program.

Most of the changes you make using the ADMIN program do not take effect until you reboot the FIREBERD 300/500. It is advisable to quit out of the ADMIN session before using any of the LAN Analyzer's other functions. Using the ADMIN session may temporarily prevent use of some of the applications due to a lockout of changing configuration via SNMP.

2.3.2 Exiting the ADMIN Program

To exit the ADMIN program, press **<F1>**. This will return you to the C:\ prompt. Quit the ADMIN session before exiting the ADMIN program.

2.4 CONNECTING THE ANALYZER TO THE NETWORK

This section describes the procedures for connecting the FIREBERD 381/581 Ethernet LAN Analyzer and the FIREBERD 383/583 Token Ring LAN Analyzer to their respective networks.

2.4.1 Connecting to Ethernet

Using 10Base5

When configuring the FIREBERD 381/581 for 10Base5 Transceiver AUI connection, you will need:

- An AUI drop cable with an appropriate 15-pin D type connector.

- A transceiver to connect the Ethernet to the drop cable.

To connect the FIREBERD 381/581 to a Standard Ethernet network, follow these steps:

1. Attach the slidelock end of the AUI Drop Cable to the transceiver on the Ethernet.
2. Attach the other end of the AUI Drop Cable to the FIREBERD 381/581.
3. Set the **SETMEDIATYPE** command in the ADMIN program to `10Base5`.

Observe these physical limits when you are installing 10Base5 cable:

- The segment length (total length of the cable path) must not be longer than 500 meters, or 1625 feet.
- Make sure there are no more than 100 stations per segment.
- Transceivers should be at least 2.5 meters, or 8 feet, apart.
- Drop cables must not be longer than 50 meters, or 162.5 feet.

Using 10Base2

When connecting the FIREBERD 381/581 to 10Base2, you will need:

- A 10Base2 T-connector.
- Thin Ethernet cables to the length required.

To connect the FIREBERD 381/581 to 10Base2, follow these steps:

1. Set the **SETMEDIATYPE** command in the ADMIN program to `10Base2`.
2. Connect the analyzer to a T-connector.

Observe the following physical limits when you are installing 10Base2:

- The segment length (total length of the cable path) must not be longer than 185 meters, or 600 feet.
- Make sure there are no more than 30 stations per segment.
- Verify that there are two properly-terminated 50Ω terminators for each segment.
- Stations should be at least 0.5 meters, or 1.5 feet, apart.

Using 10BaseT Unshielded Twisted Pair (UTP) Ethernet

When connecting the FIREBERD 381/581 to 10BaseT UTP Ethernet, you will need:

- UTP cables to the length required.

To connect the FIREBERD 381/581 to a 10BaseT UTP Ethernet, follow these steps:

1. Set the **SETMEDIATYPE** command in the ADMIN program to `10BaseT`.
2. Connect the FIREBERD 381/581 to a 10BaseT hub/concentrator.

Observe these physical limits when you are installing 10BaseT Ethernet cable:

- 24-AWG wiring is recommended, but 22-, 24-, or 26-AWG wiring may be used.
- Each point-to-point station drop must not exceed 100 meters (325 feet) between the 10BaseT station and the hub/concentrator.
- Each station drop should be free from bridge taps, and should be paired for transmit and receive.

2.4.2 Connecting to Token Ring

When connecting the FIREBERD 383/583 to a Token Ring network, you will need:

- A lobe cable with a 9-pin D connector, supplied with the FIREBERD 583.

To connect the FIREBERD 383/583 to a Token Ring network, follow these steps:

1. Connect the screwlock connector on the end of the lobe cable to the 9-pin female network connector on the FIREBERD 383/583.
2. Attach the other end of the cable to the Media Access Unit.

2.5 THE EISA CONFIGURATION UTILITY

If you add multiple test modules or change the configuration of the FIREBERD 300/500 mainframe, the mainframe has to reallocate its resources at power-up. The mainframe checks the alignment of test modules and slots. If the alignment is inconsistent with the last time the mainframe checked, you may get the following message:

```
The card in slot X does not match the EISA configuration.
```

The following line is also displayed requesting you to indicate the action to be performed.

```
Run EISA configuration utility [Y:n]
```

Press **N** if you do not want to perform the EISA configuration utility. Pressing **N** displays the `C:\` prompt.

NOTE: Uppercase letters for the selection are used only for the purpose of indicating the default selection.

Press **Y** to begin performing the EISA configuration utility.

The following sequence is performed when you press **Y** to update the EISA configuration for the current configuration.

While the EISA configuration utility is being loaded, the following message is displayed:

```
Initializing.  Please wait...
```

Then the EISA configuration utility top-level window is displayed. With this window displayed, press **<PgDn>** to highlight the step to be performed.

EISA configuration utility choices are as follows:

```
Step 1: About EISA Configuration
Step 2: Add and Remove Boards
Step 3: Change Configuration Settings
Step 4: Save Configuration
Step 5: View Switch/Jumper Settings
Step 6: Exit
```

The following steps highlight the process for updating the EISA configuration to reflect a changed mainframe configuration.

To configure the EISA utility, do the following:

1. Press **<PgDn>** to highlight `Step 2: Add and Remove Boards`.

2. Press **<Enter>**. This displays the `Step 2: Add and Remove Boards` window. If the mainframe configuration is correct, press **<Enter>**. This shows two display messages indicating that information is being read from the EISA nonvolatile memory and that it is being run in local configuration mode. After these messages appear, the Add/Remove Board window is displayed.

3. When properly configured, press **<Esc>** to return you to the EISA configuration utility top level window.

4. Press **<PgDn>** to highlight `Step 4: Save Configuration`.

5. Press **<Enter>**. The following message is displayed:

```
NOTE: Configuration data has been stored in EISA nonvolatile memory. This
configuration data will not take effect until the system is rebooted. You
may reboot the system now or exit to DOS.
Do you really want to Exit?
```

6. Press **F10** to reboot.

The following message is displayed after a successful reboot of the system:

```
EISA configuration...OK
C:\>_
```

Type `WIN` to activate Windows. In the Program Manager, click on the FIREBERD 300/500 icon to restart the FIREBERD 300/500 Test Manager.

SECTION 3
USING THE LAN ANALYZER

3.1 SECTION SUMMARY

This section describes the steps you need to take prior to using the LAN Analyzer's analysis and monitoring functions. These steps are:

- Starting the LAN Analyzer
- Using the **Analyzer** menu functions
- Loading and saving a test session
- Exiting the LAN Analyzer.

NOTE: This section assumes that you have installed the LAN Analyzer module and run the EISA configuration utility. If you haven't, refer to Section 2, Installing & Connecting the LAN Analyzer, for more information.

3.2 STARTING THE LAN ANALYZER

When you switch on the FIREBERD 300/500, the Test Manager window appears. From the Test Manager, click on the LAN icon to start the LAN Analyzer. You may also select **Interfaces>LAN:Slot x** (where **x** is the number of the slot where you've installed the LAN module) from the Test Manager menu bar. The hourglass icon momentarily appears on the screen, and the LAN Analyzer main window appears. You are now ready to set up the LAN Analyzer to start taking measurements.

3.3 USING THE ANALYZER MENU FUNCTIONS

This section shows you how to use the **Analyzer** menu functions. Use these menu functions to:

- tell the LAN Analyzer which analyzer card to use
- describe the properties of an analyzer card
- identify an analyzer card by its properties
- set up configuration and administration parameters prior to conducting the tests.

3.3.1 Adding or Deleting an Analyzer Card (Only for FIREBERD 500)

Before the LAN Analyzer can recognize an analyzer card and accept it for testing, you need to add the analyzer card to the LAN Analyzer's database. Pull down **Analyzer>New...** to add a card. When the New Analyzer box appears, enter information about this analyzer card such as its product type, and its IP Name and Name Address. Click on **OK** to add this card to the database. You will see the name of the new card displayed at the bottom of the **Analyzer** menu.

Pull down **Analyzer>Delete...** to remove the currently-selected analyzer from the database. The name will no longer be listed on the **Analyzer** menu.

3.3.2 Describing an Analyzer

After you've added an analyzer card to the database you need to provide the LAN Analyzer a description of the new card properties (including its name, product type, and IP Name and Address). You'll need to change some of these parameters from time to time while testing the network. To describe an analyzer, do the following:

1. Pull down the **Analyzer** menu, and click on the name of the analyzer card to be described. For this example, we'll use **Analyzer>Ethernet Analyzer 1**, which is a FIREBERD 581 Ethernet LAN Analyzer.

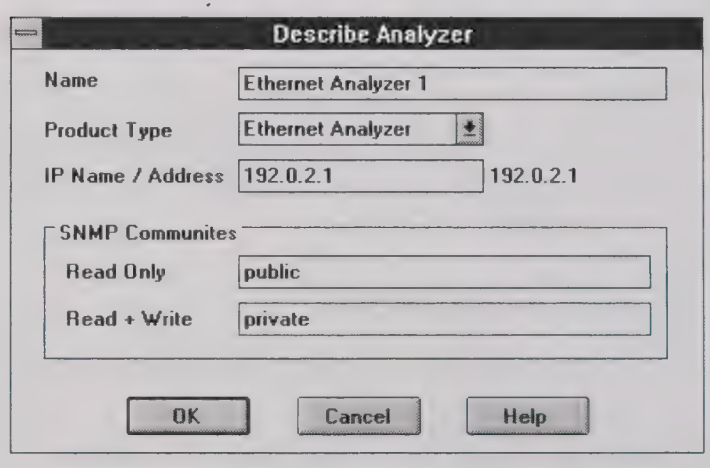


Figure 3-1
Describe Analyzer Box

2. Pull down **Analyzer>Describe...** to describe the addressing characteristics of the Analyzer. The Describe Analyzer box appears on the screen.

   NOTE: For the FIREBERD 300, the Describe Analyzer dialog box is read-only (except SNMP Communities), all the necessary information is automatically provided to user.

   Choices in the Describe Analyzer box are:

   Name — Enter a unique, descriptive name for the analyzer card, using up to 64 alphanumeric characters.

   Product Type — The choices are **Ethernet Analyzer** or **Token Ring Analyzer** card.

   IP Name / Address — Enter the IP Name and IP Address assigned to the analyzer card.

   SNMP Communities — Lets you select those community names that are permitted to read data from a device (usually **public**), and to read and write data (usually **private**). If SNMP is not supported, this box is grayed out.

3. Enter the analyzer card's name in the **Name** box.

4. Select the appropriate product type for the analyzer from the **Product Type** drop-down list. The product type for **Ethernet Analyzer 1** is Ethernet Analyzer.

5. Enter the IP Address that is assigned to the device. Since the LAN Analyzer supports SNMP, enter the appropriate SNMP Communities. Enter **Public** in the **Read Only** box, and the Analyzer will read the device's MAC address.

6. Click on **OK** to save the parameters you've entered, and exit from the Describe Analyzer box.

3.3.3 Configuring an Analyzer

Use the Configuration box to change the main properties of the current analyzer. The Configuration box appears when you pull down **Analyzer>Configure**.

Figure 3-2 shows the Configuration box.

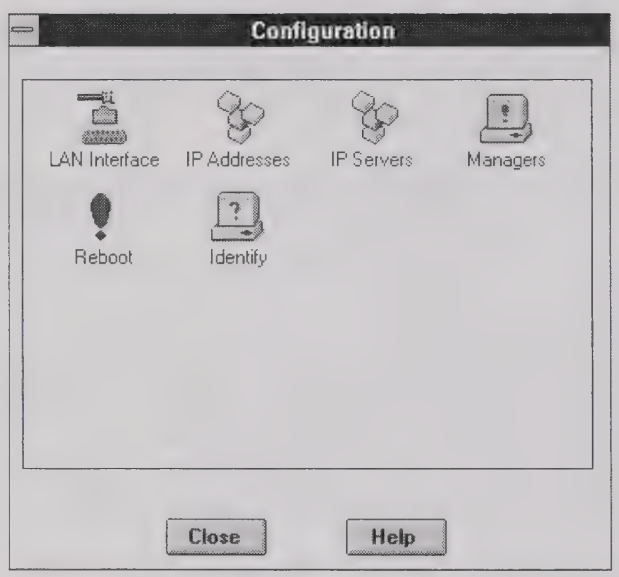


Figure 3-2
The Configuration Box

The Configuration Box

The Configuration box shows the main properties of the analyzer card you have selected. These properties are:

LAN Interface — Sets the Ethernet media type (10Base5, 10Base2, or 10BaseT) for the Ethernet analyzer, and the Ring Speed (either 4Mb/s or 16Mb/s) for the Token Ring Analyzer.

IP Addresses — Displays the current and new address, broadcast, and subnet mask for the analyzer.

IP Servers — Sets the primary and backup IP Addresses, and displays the default gateway parameters.

Managers — Displays the Management Station table for the analyzer. This table includes the IP Address, Community Name, and whether traps are enabled.

Reboot — Reboots the analyzer card you select. This clears all statistics tables and configurations.

Identify Displays a summary of information including a description of the card, the card's uptime (time, measured in hundredths of a second, since the LAN Analyzer started), the System Name, Location, and Contact person, and a listing of the Facilities Supported (a list of the components of MIB I, MIB II, and the enterprise MIBs supported by the analyzer).

The Apply Box

In each of these boxes, you have the opportunity to confirm the changes you've made to their parameters. Click on **Apply...** in any of these boxes to do this, and the Apply box appears. Figure 3-3 shows the Apply box after you've selected a different interface type in the **LAN Interface** property.

Figure 3-3
The Apply Box

Click on **Apply Selected Data** to confirm the information in the Apply box. You'll then return to the property you were in prior to clicking on **Apply...**.

3.3.4 Selecting an Analyzer (Only for FIREBERD 500)

When more than 5 analyzers are selected, the **Select Analyzer...** menu item appears at the bottom of the list of analyzers. Clicking on **Select Analyzer...** displays the Select Analyzer dialog box. From the Select Analyzer dialog box you can click on the desired analyzer to highlight it and then click on **OK** to select it as the selected analyzer.

3.4 ENDING THE LAN ANALYZER SESSION

Before you close down the LAN Analyzer, you may wish to save the test session. If you plan to use the test again, it is important to save it to a file. This section describes loading, saving, and deleting a test, ending the LAN session, and closing down the LAN Analyzer.

3.4.1 Loading, Saving, and Deleting a Test

You can take advantage of the file storage capabilities of the FIREBERD 300/500 by loading, saving, and deleting test configurations.

Loading a Test

When you load a test file, any Task that is currently running will remain running. To load an already-saved test, do these two steps:

1. Click on **File>Load Session...** and the Load Session box appears. Notice that **Load Session** in the box is grayed out.

2. Highlight the session you want to load, and click on **Load Session**.

Saving a Test

Saving a test enables you to use it for future reference. To save a test, do these three steps:

1. Click on **File>Save Session...** and the Save Session box appears. Notice that **Save Session** in the box is grayed out.

2. Enter a name for the session in the Description box. Use up to 33 alphanumeric characters. Notice that **Save Session** in the dialog box is no longer grayed out.

3. Click on **Save Session**.

Deleting a Test

Deleting a test removes it from the files. To delete a test, do these two steps:

1. Click on **File>Delete Session...** and the Delete Session box appears. Notice that **Delete Session** in the box is grayed out.

2. Highlight the session you want to delete, and click on **Delete Session**.

3.4.2 Ending the Session

When you are ready to end the session and exit the LAN Analyzer:

- You can save changes to system parameters (all the options under the **Analyzer** menu) that you have made during the session. A check mark appears next to the analyzer card in the **Analyzer** menu. To do this, pull down **File>Save Session...**. The state of these parameters is stored in the file `C:\fb500\FB500.INI`.

- Close down all running graphs and logs.

3.4.3 Closing Down the LAN Analyzer

To close down the LAN Analyzer, do any one of the following:

- Double-click on the control-menu box in the top left corner of the screen

- Click once on the control-menu box, and pull down **Close** from its menu

- Press **Alt** + **F4**.

When the LAN Analyzer closes down, you return to the Test Manager window.

SECTION 4
THE ANALYZER'S TASKS

4.1 SECTION SUMMARY

The key to the LAN Analyzer is its eleven Tasks. This section shows you what you need to do to perform tests using each Task. Included here are: accessing these Tasks, setting up a view for each one, and displaying and printing information.

4.2 ACCESSING THE TASKS

You can access any of the eleven Tasks from the LAN Analyzer main window. To access these Tasks, first pull down the **Analyzer** menu to select the analyzer card you want to use. Then, double-click on the Task's icon in the main window. For example, if you wanted to capture and decode packets, double-click on the butterfly net icon that says Capture.

4.3 USING THE HOST STATS

Use Host Statistics to collect and display statistics about the traffic transmitted and received by selected stations (hosts) on the network.

4.3.1 Setting up a Host Stats View

After you have accessed the Host Stats Task, the Statistics View Setup window appears as shown in Figure 4-1.

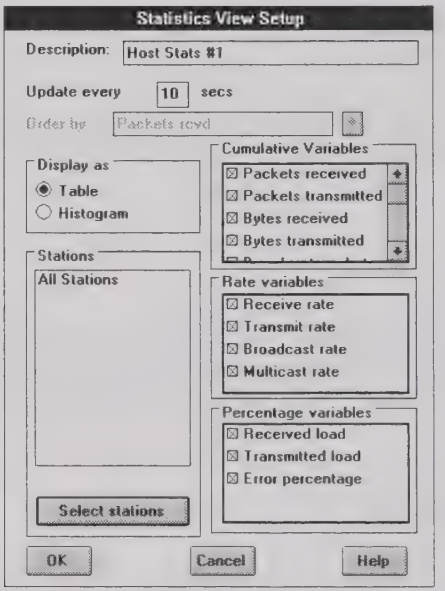


Figure 4-1
Host Statistics View Setup

The choices in this window are:

Description — Enter a descriptive name for the view you are setting up; use as many characters as you want.

Update Every — Determines how often the data in the display will be replaced with new data.

Order by — Sorts the data you collect. If you have selected `All Stations` as the data source, this field is grayed out and the data will be displayed according to the time that each station appeared on the network. If you have selected some, but not all hosts as the data sources, you can order the display according to the value of any variable in this pull-down list.

Display as — Determines whether the data is represented as a histogram or table.

Stations — Displays All Stations, which is the default station selection.

Select Stations — Click here to select the stations (hosts) to monitor the statistics, if the test requires monitoring individual stations.

4.3.2 Cumulative Variables

You may select any of the counts below for the host(s) you have selected.

Packets and Bytes

These variables are counts of either packets or bytes that are transmitted or received by the hosts you have selected. The term "octet" refers to an 8-bit entity, and is the same as a "byte". A "packet" is an Ethernet or Token Ring frame.

The full list of counts is:

Packets received	The number of packets received by the selected host.
Packets transmitted	The number of packets transmitted by the selected host.
Bytes received	The number of bytes received by the selected host.
Bytes transmitted	The number of bytes transmitted by the selected host.
Broadcast packets	The number of packets transmitted to and received by all hosts on the network. These packets have a destination address of all 1's (binary) or FFFFFFFFFFFF (hex).
Multicast packets	The number of packets transmitted to and received by a specific subset of network hosts.
Packets in error	The number of total error packets transmitted.

Error Packets

Any Ethernet packet that has a valid Frame Check Sequence (FCS) and is between 64 and 1518 bytes in length is a valid Ethernet packet. Any Token Ring packet that has a valid FCS and is between 18 and 4048 bytes in length for 4 Mb/s, or 18 and 18000 bytes in length for 16 Mb/s ring speeds, is a valid Token Ring packet. Anything else is an error packet of some sort. You may collect a count of packets in error. Error packets are also counted according to the type of error they contain:

CRC error packets	Packets with a valid length, excluding the frame bits but including the FCS, that are not an integral number of bytes or have an invalid FCS, or both.
Short packets	Packets less than the minimum bytes in length, excluding the framing bits but including the FCS. These packets otherwise are well formed.

Long packets	Packets longer than the maximum bytes, excluding the framing bits but including the FCS. These packets are otherwise well formed.
Fragment packets	Packets less than the minimum bytes long, excluding the framing bits but including the FCS that are not an integral number of bytes in length and/or have a bad FCS.
Jabber packets	Ethernet packets longer than the maximum bytes, excluding framing bits but including the FCS bytes. These packets all have a non-integral number of bytes and/or a bad FCS.

4.3.3 Rate Variables

These variables represent the number of a given type of packet per second that occurred over the last second:

Receive rate	The number of packets received by the selected host(s) during the last second.
Transmit rate	The number of packets transmitted by the selected host(s) during the last second.
Broadcast rate	The number of broadcast packets transmitted by the selected host(s) during the last second.
Multicast rate	The number of multicast packets transmitted by the selected host(s) during the last second.

4.3.4 Percentage Variables

There are two percentage variables expressing load statistics: Transmit load and Receive load. The load is represented as the percentage of network bandwidth used over the last second. Error percentage is the other percentage variable. It represents the percentage of the total packets that were error packets, over the last second.

Received load	The percentage of network bandwidth used by the selected host over the last second for receiving packets.
Transmitted load	The percentage of network bandwidth used by the selected host over the last second for transmitting packets.
Error percentage	The percentage of total packets that were error packets over the last second.

When all setup parameters are as you want them, click on **OK** to begin running the Task. The setup window is replaced by a histogram or table of the variables you have selected.

4.4 USING SEGMENT STATS

Use the Segment Statistics Task to collect and display statistics about network activity and traffic on a single segment. This section shows you how to use Segment Stats, and lists and briefly defines the available segment statistics.

4.4.1 Setting up a Segment Stats View

After you have accessed Segment Stats, the Segment Stats View Setup window appears as shown in Figure 4-2.

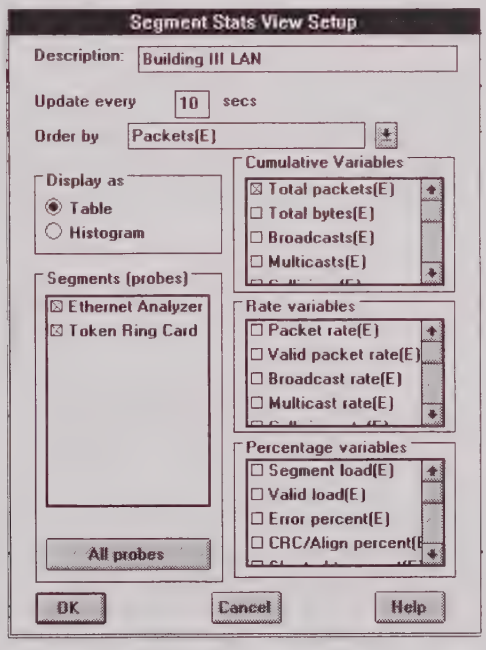


Figure 4-2
Segment Statistics Setup

The choices in this window are:

Description — Enter a descriptive tag to the set of statistical information you plan to collect with this run of the Task.

Update Every — Determines how frequently (in seconds) the data display is updated to reflect new values for the parameters you have selected.

Order by This pull-down list of ordering options sorts the data you collect.

Display as Selects whether you want the data represented as a histogram or table.

Segments Contains a list of all the analyzers on segments about which you want to collect data.

The remaining three sections in the Segment Statistics View Setup box show the various segment statistics variables according to their type. To select a variable, click on the check box to the left of the variable.

When you have the view set up as you want it, click on **OK** to run the Task. The Setup window is replaced with a data display.

Available Segment Statistics

You can access several types of segment statistics for Ethernet and Token Ring networks. Both Ethernet and Token Ring variables appear in the variable list boxes. If you select a Token Ring variable when you are testing with an Ethernet analyzer (and vice versa), the LAN Analyzer will produce a bar (—) in a table or an empty entry in a histogram.

4.4.2 Cumulative Variables

You may select any of the counts below for the segment you have selected.

Packets and Bytes

The following variables are counts of the number of either packets or bytes that are transmitted or received on the segments you have selected. The term "byte" refers to an 8-bit entity, and is also called an octet. A packet is an Ethernet or Token Ring frame. Ethernet variables are indicated by (E) and Token Ring variables by (TR).

Total packets (E)	The total number of multi-byte units of data (including error packets) received.
Total bytes (E)	The total number of octets (8 bits) of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
Broadcasts (E)	The total number of good packets received that were directed to the broadcast address.

Multicasts (E)	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Collisions (E)	The best estimate of the total number of collisions on this Ethernet segment.
64 bytes (E)	The total number of packets (including error packets) received that were 64 octets in length (excluding framing bits, but including FCS octets).
65->127 bytes (E)	The total number of packets (including error packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits, but including FCS octets).
128->255 bytes (E)	The total number of packets (including error packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits, but including FCS octets).
256->511 bytes (E)	The total number of packets (including error packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits, but including FCS octets).
512->1023 bytes (E)	The total number of packets (including error packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits, but including FCS octets).
1024->1518 bytes (E)	The total number of packets (including error packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits, but including FCS octets).
Valid packets (E)	The total number of packets (excluding error packets) received on the network.
Valid bytes (E)	The total number of octets of data (excluding those in bad packets) received on the network (excluding framing bits, but including FCS octets).
Error packets (E)	The total number of error packets received on the network.
Total packets (TR)	The total number of packets (including error packets) received on the network in the last second.
Total bytes (TR)	The total number of octets of data (excluding those in bad packets) received on the network (excluding framing bits, but including FCS octets).
Broadcasts (TR)	The total number of good packets received in the last second that were directed to the broadcast address.

Multicasts (TR)	The total number of good packets received in the last second that were directed to the multicast address. This number does not include packets directed to the broadcast address.
18->63 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 18 and 63 octets in length inclusive, excluding framing bits, but including FCS octets.
64->127 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 64 and 127 octets in length inclusive, excluding framing bits, but including FCS octets.
128->255 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 128 and 255 octets in length inclusive, excluding framing bits, but including FCS octets.
256->511 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 256 and 511 octets in length inclusive, excluding framing bits, but including FCS octets.
512->1023 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 512 and 1023 octets in length inclusive, excluding framing bits, but including FCS octets.
1024->2047 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 1024 and 2047 octets in length inclusive, excluding framing bits, but including FCS octets.
2048->4095 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 2048 and 4095 octets in length inclusive, excluding framing bits, but including FCS octets.
4096->8191 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 4096 and 8191 octets in length inclusive, excluding framing bits, but including FCS octets.
8192->18000 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were between 8192 and 18000 octets in length inclusive, excluding framing bits, but including FCS octets.
>18000 bytes (TR)	The total number of non-MAC packets (excluding packets with errors) received that were greater than 18000 octets in length, excluding framing bits, but including FCS octets.

Error Packets

Any Ethernet packet that has a valid FCS and is between 64 and 1518 bytes in length is a valid Ethernet packet. Any Token Ring packet that has a valid FCS and is between 18 and 4048 bytes in length for 4 Mb/s, or 18 and 18000 bytes in length for 16 Mb/s ring speeds, is a valid Token Ring packet. Anything else is an error packet of some sort. You may collect a count of all error packets in the cumulative variable Error packets. All of the packets included in this total are also recorded according to the type of error they contain.

Dropped packets (E) (TR)	The total number of events in which packets were dropped due to a lack of resources. This number isn't necessarily the number of dropped packets; it is the number of times that the condition was detected.
CRC errors (E)	Packets with a length between 64 and 1518 bytes, excluding the frame bits but including the FCS. These packets are either not an integral number of bytes, or they have an invalid FCS.
Short packets (E)	Packets less than 64 bytes in length, excluding the framing bits but including the FCS. These packets are otherwise well formed.
Long packets (E)	Packets longer than 1518 bytes, excluding the framing bits but including the FCS. These packets are otherwise well formed.
Fragments (E)	Packets that are not an integral number of bytes in length or have a bad FCS. These packets are all less than 64 bytes long, excluding the framing bits but including the FCS.
Jabbers (E)	Packets longer than 1518 bytes, excluding the framing bits but including the FCS bytes. These packets all have either a non-integral number of bytes or a bad FCS.
Collisions (E)	The number of collisions on the segment.

4.4.3 Rate Variables

Rate variables represent the number of a given type of packet per second that occurred over the last second.

These are the rate variables for the **Ethernet** analyzer:

Packet rate (E)	The number of packets transmitted on a given segment during the last second.
Valid packet rate (E)	The number of valid packets transmitted on a given segment during the last second.
Broadcast rate (E)	The number of broadcast packets transmitted on a given segment during the last second.
Multicast rate (E)	The number of multicast packets transmitted on a given segment during the last second.

Collision rate (E)	The number of collisions experienced on a given segment during the last second.

These are the rate variables for the **Token Ring** analyzer:

Packet rate (TR)	The number of packets transmitted on a given segment during the last second.
Broadcast rate (TR)	The number of broadcast packets transmitted on a given segment during the last second.
Multicast rate (TR)	The number of multicast packets transmitted on a given segment during the last second.
Line error (TR)	The number of packets transmitted with a bad frame check sequence.
Internal error (TR)	The number of times a Token Ring interface detected an internal error.
Burst error (TR)	The number of burst errors detected.
AC error (TR)	Address Copied error. The number of times a station on the network did not correctly recognize or copy a frame sent to it.
Abort error (TR)	The number of times a station on the network aborted transmission of a frame due to an internal error.
Lost frame (TR)	The number of times a station transmitted a frame and did not detect that it was returned.
Congestion error (TR)	The number of times a station was unable to copy a frame addressed to it due to a lack of resources.
FC error (TR)	Frame Copied error. The number of times a station detects that a frame addressed to it has already been copied by another station.
Frequency error (TR)	The number of times excessive jitter was detected in the signal.
Token error (TR)	The number of times the token is corrupted.

4.4.4 Percentage Variables

Load statistics are represented as the percentage of network bandwidth used over the last second. Error percents are the percentage of the total packets that were error packets, over the last second. You can also choose to represent the error rate according to a specific type of error.

These are the percentage variables for the **Ethernet** analyzer:

Segment load (E)	The percentage of network bandwidth used over the last second; including error packets.

Valid load (E)	The percentage of network bandwidth used over the last second by non-error packets.
Error percent (E)	Represents the percentage of the total packets which were error packets, over the last second. You can also choose to represent error rate according to a specific type of error.
CRC/Align percent (E)	The percentage of CRC or Alignment error packets to total packets received in the last second, in hundredths of a percent. CRC/Alignment error packets are packets that have a length (excluding framing bits, but including FCS octets) between 64 and 1518 bytes. These packets are either not an integral number of bytes, or they have an invalid FCS.
Short pkt percent (E)	The percentage of short packets to total packets received in the last second, in hundredths of a percent. Short packets are packets that are less than 64 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
Long pkt percent (E)	The percentage of long packets to total packets received in the last second, in hundredths of a percent. Long packets are packets that are longer than 1518 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
Fragment percent (E)	The percentage of fragments to total packets received in the last second, in hundredths of a percent. Fragments are packets that are not an integral number of octets in length or that have a bad FCS, and are less than 64 octets in length (excluding framing bits, but including FCS octets).
Jabber percent (E)	The percentage of jabbers to total packets received in the last second, in hundredths of a percent. Jabbers are packets that are longer than 1518 octets (excluding framing bits, but including FCS octets), and are not an integral number of octets in length or have a bad FCS.

These are the **Token Ring** percentage variables:

Segment load (TR)	The best estimate of the mean physical layer network utilization on this interface (excluding error frames) during the last second, in hundredths of a percent.
MAC percent (TR)	The percentage of MAC frames to total frames seen on the ring in the last second, in hundredths of a percent.
Error percent (TR)	The percentage of soft error report frames to all frames seen on the ring in the last second, in hundredths of a percent.

4.5 USING THE ALARMS

Use the Alarms Task to notify you when an event occurs, record the details of the event that triggered an alarm, and set specific thresholds for network performance.

4.5.1 The Difference Between Alarms and Events

It is important to distinguish between alarms and events. An *alarm* occurs when a threshold for the of a specific type of network event is exceeded. An *event* is something significant that happens on a network. Alarms are generated whenever the state of a device is critical or warning. The alarm is canceled when the device changes to a state other than critical or warning. When an event occurs, its details are entered in a table of Events called the Event log.

An alarm is a means of alerting you to significant network activity. Most alarms are thresholds for the occurrence of a specific type of network event. When the rate at which the event occurs (over the last second) exceeds the threshold, the alarm is triggered. You can log the alarm for future reference, and create an entry in an Event log. These logs can be accessed and viewed individually or collectively by selecting them from the Event Descriptions box in the Alarms View Setup window. The analyzer stores the information contained in the trap in the Event log. All Alarms are Events, but not all Events are Alarms.

4.5.2 Alarms View Setup

The Alarms View Setup window allows you to select one or more log tables and view them as a time-ordered list of events. Here, all of the alarms that either send an entry to the log table and/or send a SNMP trap are included. Figure 4-3 shows the Alarms View Setup.

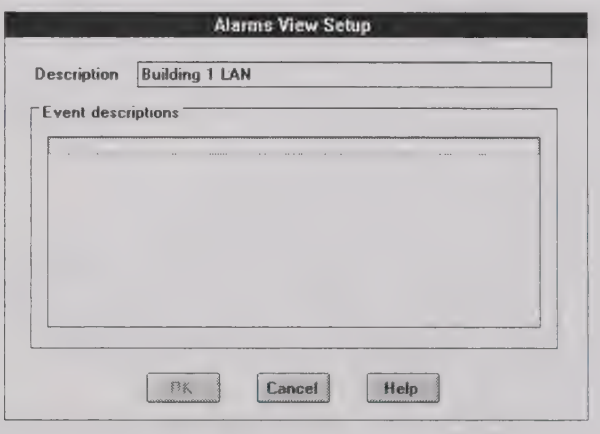


Figure 4-3
Alarms View Setup

Each entry in the list box shows the address of the network devices, followed by a description of the alarm.

To set up a view, click on the log table(s) you want to view and click on **OK**. Entries from it will be displayed in an Alarms View table, shown in Figure 4-4.

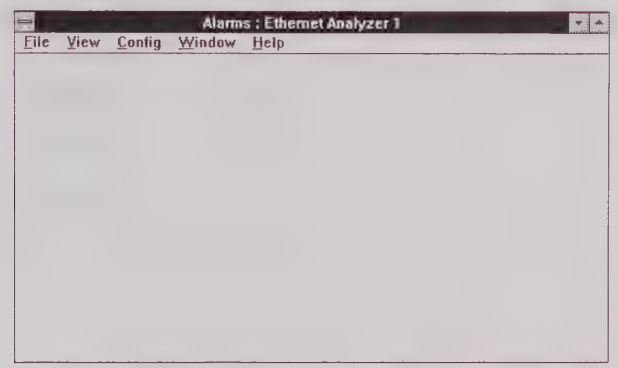


Figure 4-4
Alarms View

If you selected more than one log table from the Alarms View Setup window, the resulting view will be formed by merging these log tables in time sequence. The view contains a list box. Each row in the list box shows the time of the event (based on the FIREBERD 300/500's clock), and the log description of the event. If no alarms have occurred, the Alarms View will be empty.

4.5.3 Setting Up An Alarm

Selecting **Config>Configure Probe** brings up the Existing Alarms window, as shown in Figure 4-5.

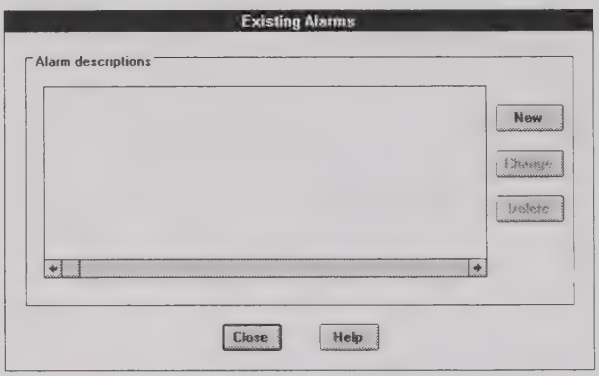


Figure 4-5
Existing Alarms Window

This window lists all of the alarms currently set. In this example, none are currently set. This section describes how to set up, change or delete an existing alarm.

Highlight the alarm and click on **Delete** to delete any of the alarms in the list. If you want to alter an existing alarm, highlight and click on it, then click on **Change** to bring back the setup window. If you want to use completely new alarms, click on **New** to bring up the Alarm Setup window as shown in Figure 4-6.

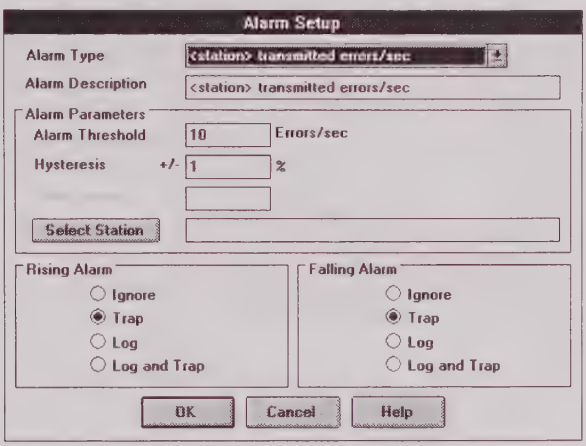


Figure 4-6
Alarm Setup

The Alarm Setup window allows you to define the parameters for a new alarm. The Alarm Setup window begins with the **Alarm Type** pulldown list, which is a list of all possible alarms that you can set up. To select an alarm from the list, click to highlight it. The **Alarm Description** field changes automatically to show the current selection in the **Alarm Type** field; you may enter your own description if you want. The box called **Alarm Parameters** also changes automatically to show only those parameters associated with the currently selected alarm type. If a parameter is grayed-out in this box, it doesn't apply to the type of alarm you have selected. When you are finished, click on **OK**.

The **Rising Alarm** and **Falling Alarm** options let you configure the alarm to trigger when the occurrence of the event first exceeds the threshold (a rising alarm), or when the occurrence of the event first falls below the threshold (a falling alarm). They also let you log an event to the alarm event log, send a SNMP trap, or log the event and send a trap. The log feature produces entries in the alarms log table.

Alarms fall into two categories: those that apply to activity on a network segment (segment-wide alarms), and those that apply to just one specified station (per-station alarms). A segment-wide or per-station alarm is triggered only when the event it monitors exceeds a pre-determined threshold. For example, a transmitted errors per second alarm for the station Orbweb is set up and shown in Figure 4-7.

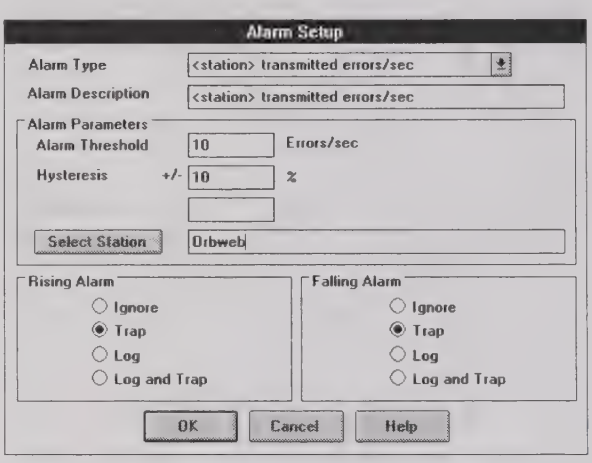


Figure 4-7
Example Setup for a Per-Station Alarm

The alarm will be triggered and logged to a file only when Orbweb transmits more than 10 error packets in any one second interval.

Alarm thresholds also have a hysteresis mechanism which limits the number of Event log entries which are generated when the value of the alarm parameter fluctuates about the threshold. Such fluctuation can result in the threshold being crossed repeatedly, causing a flood of log entries or SNMP traps being sent back to the LAN Analyzer. If you enter the percentage value 10% in the **Hysteresis** field, you effectively broaden the threshold to include any value that falls within 10% above the threshold and 10% below the threshold. No further traps are sent if the occurrence of the alarm event remains between 90% and 110% of the threshold.

When you select an alarm type, default values appear in the **Alarm Parameters** box. Since each alarm type has a reasonable default value assigned to it, you may want to leave the parameters set to the defaults until you become more familiar with this Task.

Alarm Types

You can set up a maximum of 128 alarms on any single node. There are also three categories of network alarms you can access:

Segment alarms are all configurable and pertain to a given segment.

Per-Station alarms apply only to certain selected stations and are all configurable.

New Station alarm is not a configurable alarm.

Segment Alarms

Set up any of the following alarms for individual network segments by selecting those segments one at a time. Then, configure the alarms you want and add them to the list of existing alarms for each segment.

These are the alarms available for **Ethernet** networks:

Bytes/sec
Pkts/sec
Broadcast pkts/sec
Multicast pkts/sec
CRC errors/sec
Collisions/sec
Short pkts/sec
Long pkts/sec
Fragments/sec
Jabbers/sec
Load (as a % of available bandwidth)
Error load (error packets as a percentage of total packets)
New Station detected

These are the alarms available for **Token Ring** networks:

Drop events/sec
Ring purge events/sec
Contention events/sec
NAUN changes/sec
Lost frame errors/sec
Line errors/sec

Frequency errors/sec
Burst errors/sec
AC errors/sec
Internal errors/sec
Receive congestions/sec
Frame copied errors/sec
Token errors/sec
Soft error reports/sec
Beacon events/sec
New Station detected

Per-Station Alarms

If you select a per-station type alarm from the **Alarm Type** pulldown list in the Alarm Setup window, the **Select Station** button appears in the **Alarm Parameters** section. Click on this button to bring up the **Select Stations** window, shown in Figure 4-8.

The Select Stations window has a scroll-through list of all available stations. To select one, highlight it and double-click on it, or highlight, or click on **Add**. The station then appears in the **Stations selected** section. To select all stations on the segment, click on **All stations**. If you want to remove a station from the **Stations selected** list, highlight it and click on **Delete**, or click on **Delete all** to remove all of the selected stations.

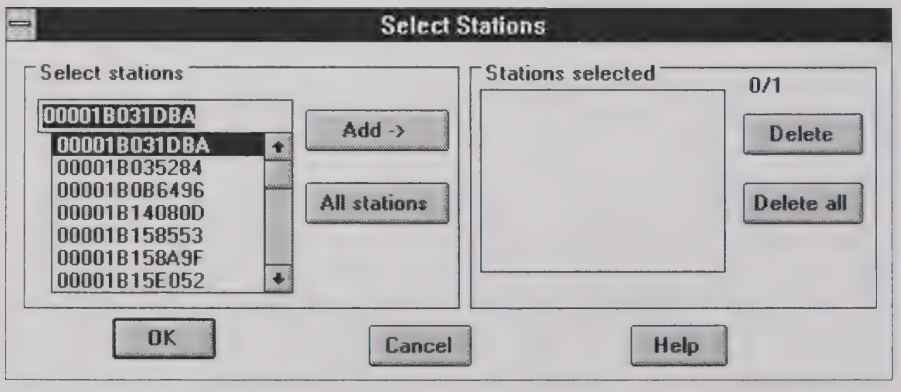


Figure 4-8
Select Stations

The per-stations alarms for **Ethernet** networks are:

Transmitted pkts/sec
Received pkts/sec
Transmitted bytes/sec
Received bytes/sec
Transmitted errors/sec
Transmitted broadcasts/sec
Transmitted multicasts/sec
Transmitted load
Received load
Error load
Stops transmission (for some specified number of seconds)

The per-stations alarms for **Token Ring** networks are:

Transmitted pkts/sec
Received pkts/sec
Transmitted bytes/sec
Received bytes/sec
Transmitted errors/sec
Transmitted broadcasts/sec
Transmitted multicasts/sec
Transmitted load
Received load
Error load
Stops transmission
Received duplicate addresses/sec
Received line errors/sec
Transmitted line errors/sec
Internal errors/sec
Received burst errors/sec
Transmitted burst errors/sec
Received AC errors/sec
Received abort errors/sec
Received lost frame errors/sec
Received congestion errors/sec
Received FC errors/sec
Received frequency errors/sec
Received token errors/sec
Received beacon errors/sec
Transmitted beacon errors/sec
Insertions/sec

New Station Alarms

This alarm indicates a new station has appeared on the segment. It is the only alarm that has no threshold to set. When this alarm is triggered, use the Event Browser to find the name of the new stations; refer to Section 5.2, Events and The Event Browser. The Event log shows you if there is more than one new station.

4.6 USING MATRIX STATS

Use the Matrix Statistics Task to examine the incoming and outgoing traffic on a segment, to compile lists of the MAC addresses for all stations that send or receive traffic, and determine the percentage of bandwidth that the stations are consuming.

4.6.1 Setting Up a Matrix Stats View

The Matrix Statistics Task requires very little configuration. After you have accessed the Matrix Stats Task, the Select View Type window appears as shown in Figure 4-9.

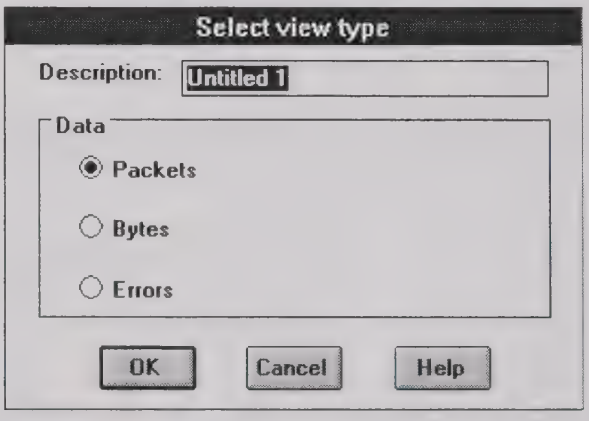


Figure 4-9
Matrix Statistics Select View Type

The choices in this window are:

Description — The title of the data display consists of up to 39 alphanumeric characters. You may want to make it specific in order to distinguish it from other displays that you may be viewing at the same time.

Packets, Bytes, Errors — Determines the nature of the traffic you want to display.

When you have set up the parameters, click on **OK** to begin running the test. Figure 4-10 shows the Matrix Stats display.

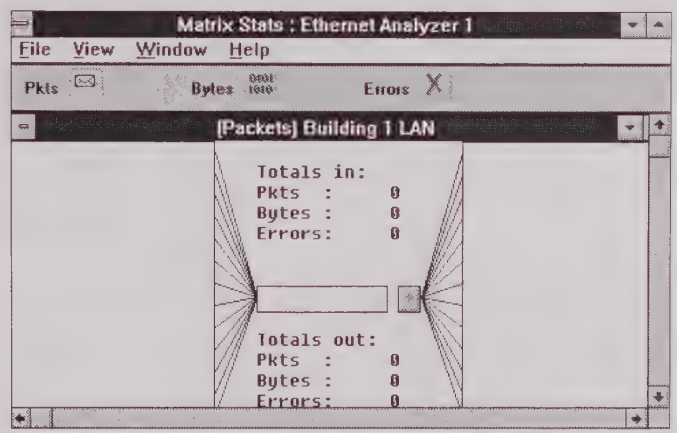


Figure 4-10
Matrix Stats Display

Initially, the display appears empty. The section on the left side of the display contains the list of devices (such as bridges, routers, or terminals) that have sent packets to the designated station; the section on the right contains the list of devices that received traffic from the designated station.

There are two sets of statistics totals appearing in the middle section: `Totals in:` is for traffic received by the designated station; `Totals out:` for traffic transmitted by the designated station. Note that there are total counts for packets in/out, bytes in/out, and errors in/out regardless of which parameter you selected in the Setup window. Large numbers are expressed in scientific notation: 2.5104e+005 means 2.5104 times 10 raised to the fifth power. Initially, all of these figures are zero.

The middle section contains a scroll-box listing all devices that can be seen. Click on the down arrow to pull down the list. If you expand the display window by dragging its borders outward, the scroll-box expands to display more stations. Use the scroll bar to move up and down the list. Note that the list has been processed automatically by the Address Translation Table. Designate the station about which you want statistics by clicking on it; the address/name of the selected station appears in the box above the list.

The hourglass icon will appear for a few seconds while the LAN Analyzer gathers information. Then the lists will appear in the left and right sections, and the figures in the center section will be updated. Figure 4-11 depicts the Matrix Stats Packet Data display.

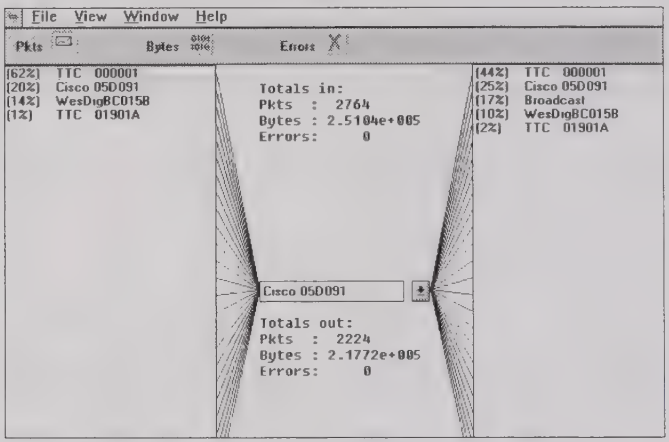


Figure 4-11
Matrix Stats Packet Data

Each station in the incoming traffic section has a percentage figure listed after it. The figure represents the proportion of the total incoming traffic sent by that station. In the example shown in Figure 4-11, the device named **`WesDigBC0158`** contributed 14% of all packets sent to the designated station **`Cisco05D091`**. Each station in the outgoing traffic list also has a percentage figure listed after it, representing the proportion of the total outgoing traffic received by that station. In this example, **`WesDigBC0158`** received 10% of the packets transmitted by the designated station.

Stations are listed according to the percentage of traffic they transmitted or received, ordered from most to least. All percentages are rounded to the nearest whole number.

4.6.2 Changing the View

You can change the view without returning to the Setup window, using the **Pkts**, **Bytes**, and **Errors** buttons in the Toolbar. Click on these to switch the type of data displayed for the designated station.

To start a new view, pull down **View>New**, then use the Setup window to describe the new view.

4.7 USING PACKET CAPTURE

Use the Capture Task to capture and decode the packets transmitted and received by hosts on the network. This Task is very powerful and has more than one setup screen for you to edit. When you select Capture, you filter certain types of "live" packets out of network traffic and store copies of them in a buffer. The analyzer then decodes the captured packets and displays their contents. You can also use this Task to decode and display the contents of captured packets that have been saved in disk files. You can run separate Capture applications simultaneously so you can compare traffic on different network segments.

4.7.1 Filters and Triggers

The LAN Analyzer uses a *Filter*, or a combination of filters, to define which packets are to be captured. A filter is simply a blank packet that you edit to create a "description" of the type of packet to be captured. When you combine several filters, you can create an overall description that can include several types of packets and specifically exclude others. Each packet is compared against the filter(s). If the packet matches the description established by the filter(s), the packet is sent either directly to the capture buffer or to one of three triggers.

Triggers define the start and stop conditions for packet capture. When a packet matches a filter connected to a trigger, the LAN Analyzer either begins or stops capturing packets, depending on how you have defined the triggers. You specify the path the packet follows by connecting the filter(s) either directly to the capture buffer or to the triggers.

When capture is completed, the LAN Analyzer decodes the contents of the captured packets and you can display them in a variety of ways and formats.

4.7.2 Setting Up Views to Capture Packets

The Capture Task follows standard Windows procedures such as point and click. To capture the data, follow these steps:

1. Access the Capture Task.
2. From the **Configure** menu, select **Load from Probe**.
3. Describe the packet to be captured, and select a filtering template type.
4. Set up the template. Be specific in setting up filters, because each filter describes a packet.
5. Draw the filtering scheme, then capture LAN traffic.
6. View the decoded packets.

After you have accessed the Capture Task, the Capture window appears, as shown in Figure 4-12.

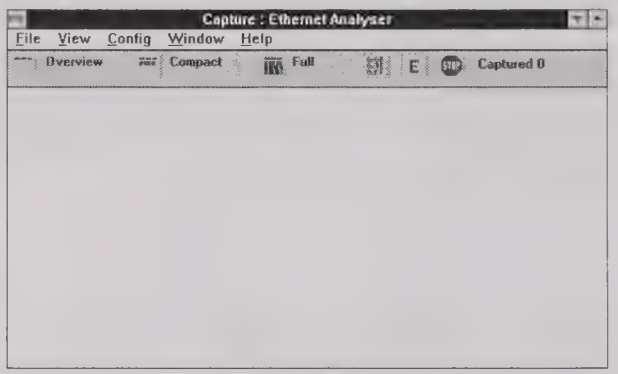


Figure 4-12
Capture

4.7.3 Setting Up Capture

To set up the Task, click on **Config** in the menu bar and select the configuration source. Both **Load from Probe** and **Load from File** are selectable, even if no configurations are saved to a file. Note that there are no files listed in the **Load from File** window until you've saved a configuration. The next display you will see is the Capture Setup window, as shown in Figure 4-13.

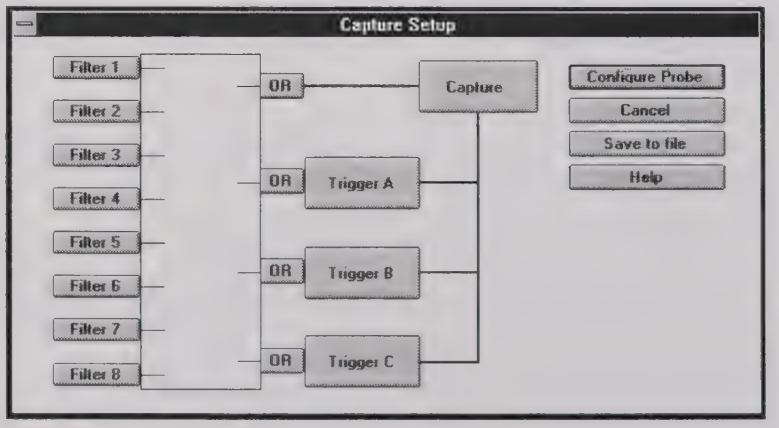


Figure 4-13
Capture Setup

Down the left side of the display you see the filters (1 through 8). The three triggers (A through C) are in the center of the window; between the filters and triggers are the **OR/NOT** boxes. (Click on **OR** to change the box from **OR** to **NOT** and vice versa.) The capture conditions are represented by the **Capture** box, located above and to the right of the **Trigger A** box. Setting up filters, triggers using **OR/NOT** boxes, and capture conditions are described separately in the following sections.

The Ethernet or Token Ring analyzer determines the template displayed when you click a **Filter** box. If you're testing with an Ethernet card, clicking on **Filter** displays the MAC Level Template. However, if you're testing with a Token Ring card, clicking on **Filter** displays the MAC and LLC Level Template. See the following subsections for more information.

4.7.4 Setting Up Filters for Ethernet

Each packet transmitted over a segment is compared with one or more of the filters represented in this window. Any packet that matches a filter is then either sent directly to the capture buffer or sent to a trigger, depending on the path you establish in this window.

The MAC Level Template

To set up a filter defining the type(s) of packet you want to capture, click on a filter in the Capture Setup window. The MAC Level Template for an Ethernet network is shown in Figure 4-14.

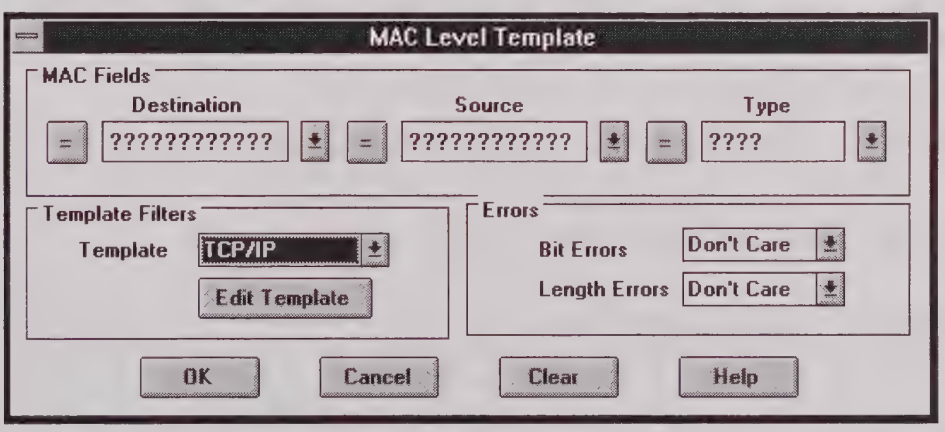


Figure 4-14
MAC Level Template

Descriptions of the parameters in this template are listed below. **Template Filters** displays the selected template. Clicking on the arrow next to **Template** displays the Template choices. Template choices are **TCP/IP**, **Hex**, **ISO**, and **NetWare**. The Template type you choose determines the Filter Template window displayed when you click on **Edit Template**.

The **Errors** field displays two types of errors: **Bit Errors** and **Length Errors** and the current selection for each. **Errors** lets you specify whether you want to capture all packets that match the filter including error packets, only valid packets, or only packets that contain certain types of errors.

Bit Errors	Lets you set up the filter to match packets containing CRC/Alignment errors.
OK	Capture only packets that do not contain CRC/Alignment errors.
CRC/Align	Capture only packets that either are a non-integral number of bytes in length or have an invalid FCS.
Don't Care	Consider any packet to be matched with this field.
Length Errors	Lets you state the preferences about packet length errors.
OK	Capture only those Ethernet packets that do not contain packet length errors.
Short	Capture only packets that are less than 64 bytes in length but are otherwise well formed.
Long	Capture only those Ethernet packets that are longer than 1518 bytes but are otherwise well formed.
Don't Care	Consider any packet to be matched with this field.

NOTE: Buttons marked **!=** next to some fields let you perform a logical NOT on the field.

4.7.5 Setting Up Filters for Token Ring

MAC and LLC Level Template

Let's look at how filters are set up to define the type(s) of Token Ring packet(s) you want to capture. To set up a filter, click on one of the eight filters. The MAC (Media Access Control) and LLC (Logical Link Control) Level Template is displayed as shown in Figure 4-15.

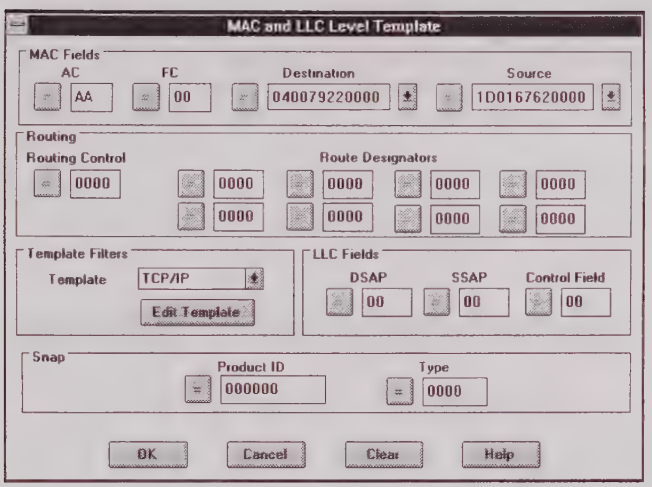


Figure 4-15
MAC and LLC Level Template

Descriptions of the parameters in this template are listed below. The Template Filters window displays the selected template. Clicking on the arrow next to the **Template** field displays the Template choices. Template choices are **TCP/IP**, **Hex**, **ISO**, and **NetWare**. The Template type you choose determines the Filter Template window displayed when you click on **Edit Template**.

The following choices are available:

MAC fields:

AC	Access Control.
FC	Frame Control.
Destination	Address of the host receiving the packet.
Source	Address of the host sending the packet.

Routing:

Routing Control **Route Designators**	Optional. Necessary only when packets are generated from outside the source ring. If this is the case, enter data from the **Routing Control** field and up to eight 2-byte **Route Designators**.

LLC Fields:

DSAP **SSAP** **Control Field**	In the **DSAP**, **SSAP**, and **Control Field**, enter the data to define the complete LLC. The **PDSAP** and **SSAP** address fields refer to the service access points that interface the network and link layers. The **Control Field** indicates that the generated packet will be one of three types: information, supervisory, or unnumbered packet.

Snap:

Product ID	802.5 networks use SNAP to encapsulate Ethernet packets. Enter the **Product ID** and **Type** in the fields provided.
Type	

4.7.6 The TCP Filter Template - An Example

Selecting TCP/IP as the Template and clicking on **Edit Template** displays the TCP Filter Template, as shown in Figure 4-16.

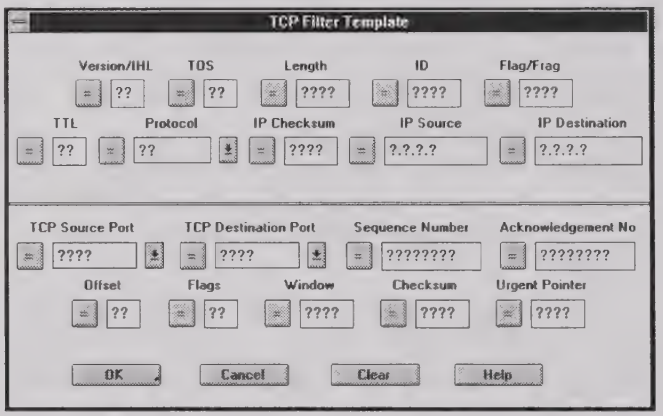


Figure 4-16
TCP Filter Template

The following choices are available on the TCP Filter Template:

Version/IHL	Indicates the Version (4 bits) and the Internet Header Length (4 bits). Version indicates the format of the Internet header. IHL indicates the length of the Internet header in 32-bit words, thus pointing to the beginning of the data. The minimum value for a correct header is 5.
TOS	Indicates the Type of Service (8 bits). TOS indicates the parameters of the quality of service desired. This includes the precedence, delay, throughput, and reliability.
Length	Indicates the total datagram length (16 bits) measured in octets, including the Internet header and data.
ID	Indicates the identification (16 bits). This is the identifying value assigned by the sender to aid in assembling the fragments of a datagram.

Flag/Frag Indicates the Flags (3 bits) and Fragment Offset (13 bits). The 3 flag bits indicate whether the datagram may be fragmented or not and whether it is the last fragment or more fragments are following. The fragment offset indicates where in the datagram this fragment belongs. Fragment offset is measured in units of 8 octets (64 bits), with the first fragment having an offset of 0.

TTL Indicates the Time to Live (8 bits). This is the maximum time the datagram is allowed to remain in the Internet system; TTL is the upper bound on the time a datagram may exist. When this value is 0, the datagram is destroyed.

Protocol Indicates the next level protocol used in the data portion of the Internet datagram.

Protocol choices include:

??	Wildcard, all protocols
ICMP	Internet Control Message Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ISO-TP4	ISO Transport Protocol Class 4
IGMP	Internet Group Management Protocol
GGP	Gateway to Gateway Protocol
ST	Stream Protocol
ULC	University College London Protocol
EGP	Exterior Gateway Protocol
IGP	Interior Gateway Protocol
BBN-RCC-MON	BBN RCC Monitoring
NVP-II	Network Voice Protocol
PUP	PARC Universal Packet Ethertype
ARGUS	ARGUS Protocol
EMCON	Emission Control Protocol
XNET	Cross Net Debugger
CHAOS	CHAOS Protocol
MUX	Multiplexing Protocol
DCN-MEAS	DCN Measurement Subsystems Protocol
HMP	Host Monitoring Protocol
PRM	Packet Radio Measurement
XNS-IDP	Xerox NS IDP
TRUNK-1	Trunk-1 Protocol
TRUNK-2	Trunk-2 Protocol
LEAF-1	Leaf-1 Protocol
LEAF-2	Leaf-2 Protocol
RDP	Reliable Data Protocol
IRTP	Internet Reliable Transaction Protocol
NETBLT	Bulk Data Transfer Protocol

Protocol choices include:

MFE-NSP	MFE Network Services Protocol
MERIT-INP	MERIT Internodal Protocol
SEP	Sequential Exchange Protocol
SFTP	Simple File Transfer Protocol
SAT-EXPAK	Satnet and Backroom EXPAK
MIT-SUBNET	MIT Subnet Support
RVD	Remote Virtual Disk Protocol
IPPC	Internet Pluribus Packet Core
SAT-MON	SATNET Monitoring
IPCU	Internet Packet Core Utility
BR-SAT-MON	Backroom SATNET Monitoring
WB-MON	Wideband Monitoring
WB-EXPAK	Wideband EXPAK

IP Checksum The header checksum is recomputed and verified at each point that the Internet header is processed.

IP Source Indicates the Source Address (32 bits). This is the IP address of the host sending the datagram.

IP Destination Indicates the Destination Address (32 bits). This is the IP address of the host receiving the datagram.

TCP Source Port Indicates the source port number (16 bits).

TCP Source Port choices include:

????	Wildcard
REXEC	Remote UNIX host command execution (password required)
RLOGIN	Login using the UNIX security scheme
RSH	Connects to a specified UNIX host
LPR	Line Printer Remote
FTP-DATA	File Transfer Protocol Data
FTP	File Transfer Protocol
TELNET	Telnet Protocol
SMTP	Simple Mail Transfer Protocol
DOMAIN	Domain Name Service
BOOTPS	Bootstrap Protocol Server
BOOTPC	Bootstrap Protocol Client
TFTP	Trivial File Transfer Protocol
ISO-TSAP	ISO TSAP
SUNRPC	SUN Remote Procedure Call

TCP Source Port choices include:

RJE	Remote Job Entry
ECHO	Echo Protocol
DISCARD	Discard Protocol
USERS	Active Users Protocol
DAYTIME	Daytime Protocol
QUOTE	Quote of the Day Protocol
CHARGEN	Character Generator Protocol
NSW-FE	NSW User System Front End
MSG-ICP	MSG ICP Protocol
MSG-AUTH	MSG Authentication Protocol
DSP	Display Support Protocol
TIME	Time Server Protocol
RLP	Resource Location Protocol
GRAPHICS	Graphics Protocol
NAMESERVER	Host Name Server
NICNAME	Who Is Protocol
MPM-FLAGS	MPM Send Protocol
MPM	Internet Message Protocol (Multimedia Mail)
MPM-SND	MPM Send Protocol
NI-FTP	NI File Transfer Protocol
LOGIN	Login Host Protocol
LA-MAINT	IMP Logical Address Protocol
ISI-GL	ISI Graphics Language Protocol
NI-MAIL	NI Mail Protocol
VIA-FTP	VIA Systems-File Transfer Protocol
TACAS-DS	TACAS-Database Service
NETRJS-1	Remote Job Service 1
NETRJS-2	Remote Job Service 2
NETRJS-3	Remote Job Service 3
NETRJS-4	Remote Job Service 4
FINGER	Finger Protocol
HOSTS2-NS	Host2 Name Server
MIT-ML-DEV	MIT ML Device
SU-MIT-TG	SU/MIT Telnet Gateway Protocol
MIT-DOV	MIT Dover Spooler
DCP	Device Control Protocol
SUPDUP	SUPDUP Protocol
SWIFT-RVF	Remote Virtual File Protocol
TACNEWS	TAC News
METAGRAM	Metagram Relay
HOSTNAME	Hostname Protocol

TCP Source Port choices include:

X400	X.400
X400-SND	X400-SND
CSNET-NS	CSNET Mailbox Nameserver Protocol
RTELNET	Remote Telnet Service
POP-2	Post Office Protocol - Version 2
AUTH	Authentication Service
SFTP	Simple File Transfer Protocol
UUCP-PATH	UUPC Path Service
NNTP	Network News Transfer Protocol
ERPC	Encore Expedited Remote Protocol Call
NTP	Network Time Protocol
LOCUS-MAP	LOCUS PC-Interface Network Map Service
LOCUS-CON	LOCUS PC-Interface Network Connection Service
PWDGEN	Password Generator Protocol
CISCO-FNA	CISCO FNATIVE
CISCO-TNA	CISCO TNATIVE
CISCO-SYS	CISCO SYSMAINT
STATSRV	Statistics Service
INGRES-NE	INGRES-NET Service
LOC-SRV	Location Service
PROFILE	Profile Naming System
NETBIOS-NS	NETBIOS Name Service
NETBIOS-DGM	NETBIOS Datagram Service
NETBIOS-SSN	NETBIOS Session Service
EMFIS-DATA	EMFIS Data Service
EMFIS-CNTL	EMFIS Control Service
BL-IDM	Britton Lee Intelligent Database Machine
SUR-MEAS	Survey Measurement
LINK	Link Protocol

Sequence number The sequence number of the first data octet in this segment (32 bits).

Acknowledgment No Indicates the value of the next sequence number the sender of the segment is expecting to receive, if the ACK control bit is set (32 bits).

Offset Data Offset indicates the number of 32-bit words in the TCP Header (4 bits). This indicates where the data begins. The TCP Header is an integral multiple of 32 bits.

Flags Indicates whether or not the datagram is fragmented, and whether it is the last fragment or more fragments are following.

Window Indicates the number of data octets beginning with the one indicated in the acknowledgment field, which the sender of this segment is willing to accept (16 bits).

Checksum Indicates the 16-bit 1's complement of the 1's complement sum of all 16-bit words in the header.

Urgent Pointer Indicates the current value of the urgent pointer as a positive offset from the sequence number in this offset (16 bits). The urgent pointer points to the sequence number of the octet following the urgent data.

4.7.7 Destination, Source, Type, Data, and Invert Fields

Destination and Source

At the MAC level template, you can use the **Destination** and **Source** fields to set up the filter to match only those packets transmitted to or from specific stations. Click on the arrow to display the list of stations that the analyzer can "see". To select a station, click on its name or address. If you want to ignore the source or destination of the packet when comparing it to the filter, set these fields to **All Stations** or to wildcards (**???????????**); then the analyzer will consider a packet's source or destination to be matched with the filter regardless of which station sent or received it.

Type

Every Ethernet packet has a 2-byte **Type** field that the Ethernet driver at the packet's destination address uses to direct the packet up to the appropriate protocol module. If you don't care which protocol module a packet is bound for, leave this field set to wildcard (**????**). At the MAC Level template, you may select any of these packet types:

TCP/IP	Transmission Control Protocol/Internet Protocol
ARP	Address Resolution Protocol
AARP	Apple Address Resolution Protocol
APPLETALK	Apple Computer's Ethernet
NETWARE1	Novell's NetWare 1
NETWARE2	Novell's NetWare 2
MOP1	Maintenance Oriented Protocol 1
MOP2	Maintenance Oriented Protocol 2
DECNET	Digital Equipment Network
LAT	Local Area Transport Protocol
LAVC	DEC LAVC
Banyan1	Banyan VINES 1
Banyan2	Banyan VINES 2
NBP	Name Binding Protocol

If you are using the TCP/IP template, you may choose either TCP/IP or wildcard.

Data

Initially, the remaining fields are filled with either text or wildcards. The wildcards mean "anything". When a packet is compared to this filter, the LAN Analyzer considers all of the filter's wildcard fields as matched with the corresponding packet fields, regardless of what the packet fields actually contain. Click on a field to select it, or double-click to edit it. An arrow box indicates a hidden list of values; click on the arrow to display the list. Change the value of a field by overwriting the current value or by selecting a value from the pull-down list. Any field that is irrelevant to the type of packet you want to capture should be left as a wildcard. Click on **Clear** to set all fields to wildcards.

Invert

In some cases, you will need to design a filter so that any packet that doesn't match certain fields is captured. For example, suppose you want to capture all TCP/IP packets transmitted by a specific host that are not UDP packets. Using the TCP/IP Template, set the **Source** to the host's name (or address), set the **Type** to TCP/IP, and the **Protocol** to UDP, and invert the field to create a logical NOT for a field. To do this click the **=** or **!=** button to the left of the field. Select the field you want to invert (the **Protocol** field in our example above) by clicking on it, entering a value, then click on the field. You can tell a field has been inverted by looking at the symbol; the **=** symbol indicates a normal field and the **!=** symbol denotes an inverted field. If you change your mind about a field you have inverted, click on the field again. Inverting wildcard fields has no effect at all on the filter.

When you have finished setting up the filter, click on **OK**; the window closes and returns to the Capture Setup window. If you need to set up additional filters, click on the appropriate filter button in this window and repeat the filter setup process.

4.7.8 Combining Filters

You can combine several filters to create a complex description of the packets you want to capture. This is necessary when you want to capture only packets of several distinct types. You can define a filter for each of these types and then combine the filters by connecting them all to the same trigger, or sending them all directly to the capture buffer.

To connect several filters to the same trigger or to the capture buffer, draw a line from each filter to the appropriate **OR/NOT** box (by clicking on the short line on the right side of the filter, holding down the mouse button while dragging the line over to the short line on the left side of the **OR/NOT** box, then releasing the mouse button). To delete an existing line, draw over it. The lines you draw establish the path followed by a packet that has been matched with a filter. Note that you cannot connect a filter to more than one **OR/NOT** box. Consider the Capture Setup window shown in Figure 4-17.

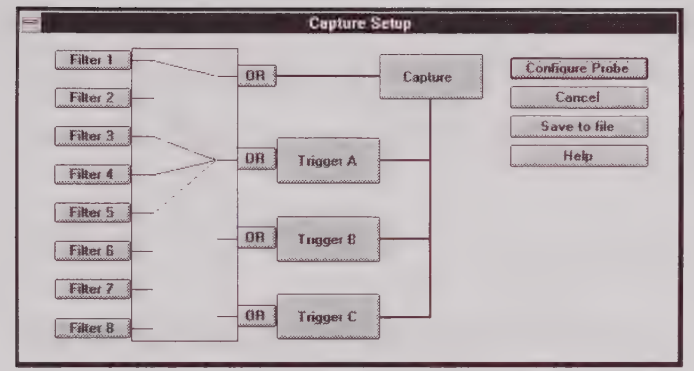


Figure 4-17
Combining Filters

In this example, any packet that matches **Filter 2** or **Filter 3** or **Filter 4** or **Filter 5** is passed on to Trigger A, which might be set up to start capture. Any packet matching **Filter 1** will be captured until the capture buffer is full, or you stop Capture manually.

You can also combine filters by NOT-ing them together. Click on an **OR** box to change it to **NOT**. If we had NOTed together the four filters in the example above, any packet that does not match any of Filters 2 through 5 would be passed on to Trigger A. That is, if a packet did match even one of the filters, it would not be passed on.

You can create quite elaborate combinations of filters by using the **OR/NOT** boxes along with the **Invertfield** feature for filter setup. If you invert every field in a filter as you set it up, you effectively create a NOT for the entire filter. This allows you more flexibility in creating filter combinations.

4.7.9 Using Triggers - An Example

Let's consider an example using triggers, as shown in Figure 4-18. Suppose you want to:

- Begin Capture when the analyzer detects a packet that initiates a workstation's connection to station Host_1.
- Capture all subsequent packets sent between station Host_1 and station Host_2 until the connection to station Host_1 is closed.

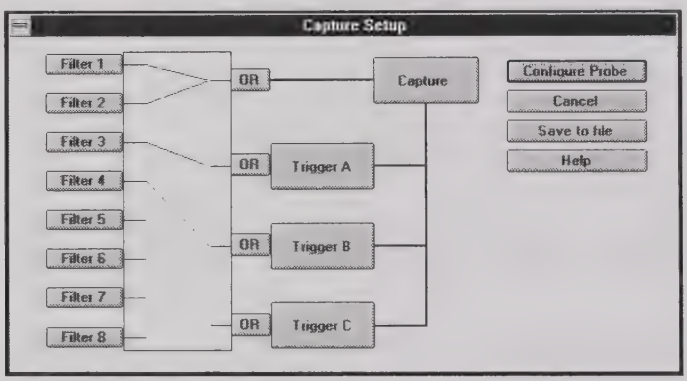


Figure 4-18
Example Using Triggers

To set up four filters:

1. **Filter 3** is set up to match a packet that initiates a connection between the workstation and station Host_1.
2. **Filter 1** is defined as "any packet with **Source** Host_1 and **Destination** Host_2"; **Filter 2** is defined as "any packet with **Source** Host_2 and **Destination** Host_1".
3. **Filter 4** is set up to match a packet that closes the connection between the workstation and station Host_1.

You establish the path between the filters and the triggers and the **Capture** box:

1. Draw a line connecting **Filter 3** to **Trigger A**.
2. Draw another line connecting **Filter 4** to **Trigger B**.
3. Connect **Filter 1** and **Filter 2** directly to the **Capture** box.

4. Click on the **Capture** box and set to **Capture on trigger**.

5. Set **Trigger A** to **Start Capture** and **Trigger B** to **Stop Capture**, then click on **OK**.

   NOTE: The packet that trips a trigger is not passed on to the capture buffer.

4.7.10 Using a Trigger to Count Packets

A trigger can also be used to count the number of packets that pass through it. Click on **Trigger A**. The display will look like Figure 4-19.

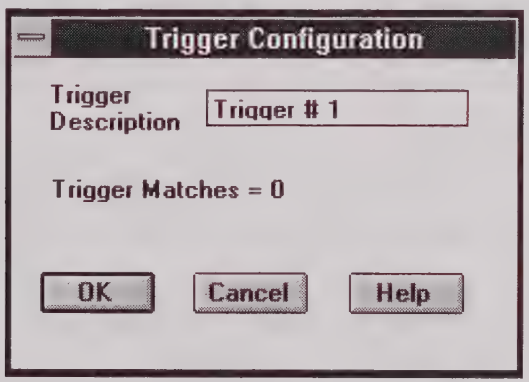


Figure 4-19
Trigger Information

There is a **Trigger Description** field for you to enter a brief description of the trigger. This can be up to 128 alphanumeric characters in length. **Trigger Matches** is a counter. The value of this field represents the number of packets that pass through this trigger. If you have connected just one filter (which matches only one type of packet) to a trigger, the **Trigger Matches** choice acts as a counter for this type of packet.

4.7.11 Starting and Stopping Capture

Starting Capture

Click on the **Capture** box in the Capture Setup window. Here, you can specify whether capture will start immediately or on a trigger. If you want to start capture on a trigger, you must indicate **Capture on trigger** and specify which one. To do this, simply click on the appropriate button, as shown in Figure 4-20. **Capture immediately** overrides any triggers that are used to start or stop capture. Click on **OK** to return to the Capture Setup window.

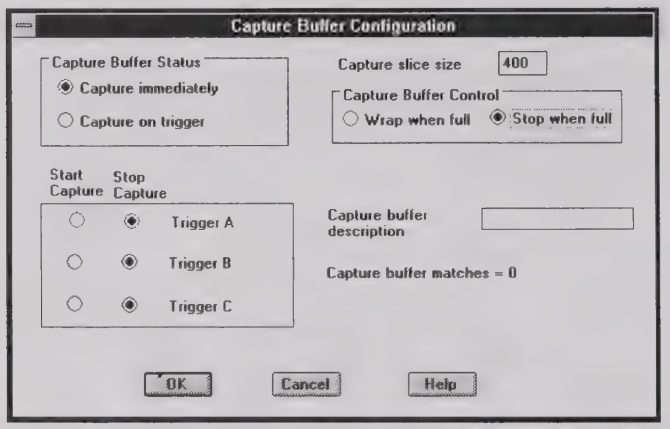


Figure 4-20
Capture Box Display

Click on **Configure Probe** to begin capturing packets. The Capture Setup window will be replaced by the capture display.

Stopping Capture

You can use a trigger to stop capture. As we noted earlier, there are other ways to accomplish this. The **Capture Buffer Control** section contains two options. If you select **Stop when full**, packet capture will continue until the buffer contains the maximum number of packets it can hold. This number will vary, depending upon the size of the captured packets. If you select **Wrap when full**, capture will continue until it is stopped either manually or by a trigger; when the buffer is full, the analyzer will start overwriting the least recently captured packets with the most recent.

To stop capture manually, go to the Capture window and click on **STOP** in the Toolbar. Or, pull down **View>New View**, then click on **OK** in the dialog box; this will stop capture and begin displaying captured packets.

4.7.12 Capture Slice Size

Capture slice size lets you specify the first *n* bytes of each packet you want to capture. You may capture up to 1518 bytes of each packet. The slice size affects the total number of packets that can be saved in the buffer; a large slice size results in fewer saved packets. The default value is 400 bytes. If you are interested primarily in the information contained in packet headers, using a small slice size allows you to save more packets in the buffer, while still allowing you to display all of each packet's relevant information.

NOTE: Slicing off part of a packet may cause problems with decodes that check, for example, the length of the packet. You may see an error message reporting this. If this is the case, it may mean that the whole packet is not decoded; only part of it may be displayed in Hex form.

Capture Buffer Description

This field lets you add a helpful descriptive label to the collective contents of the capture buffer stored in the probe.

4.7.13 Capture Buffer Matches

Capture buffer matches indicates the number of packets that matched the filters you have configured.

When you have finished setting up this window, click on **OK**. This returns you to the Capture Setup window; click on **Configure Probe** to begin packet capture.

4.7.14 Saving Capture Configurations

If you frequently use more than one capture setup, you can save the configuration to a file and recall it whenever you need it. To do this:

1. Configure your Capture Setup screen.
2. Click on **Save to file**.
3. Enter a name for your configuration in **Description** and click on **Save Config**.

   RESULT: Your configuration is now saved.

You can recall your saved configuration by choosing **Config>Load from File** from the menu bar. You can delete the configuration by choosing **Config>Delete Config File** from the menu bar.

The way you save a display configuration determines how the data will be displayed when **View Load** is clicked on. Clicking on **View Load** actually loads the view, not the data. The data is saved by clicking on **File>Save as**.

4.7.15 Displaying Packets

Once capture has started, you can begin displaying the packets in the capture buffer. It is worth noting that when scrolling through packet displays, there may be occasional delays while the analyzer loads up the data. From the Capture window menu bar, pull down **View>New View...**. Figure 4-21 depicts the New View Configuration window.

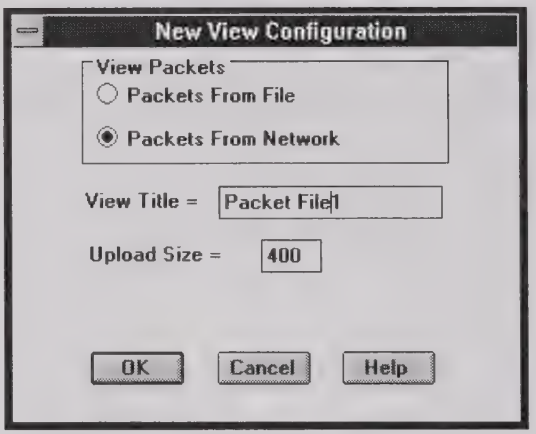


Figure 4-21
Setting Up Packet Display

The **View Packets** section offers you two choices. To view the packets in the Capture buffer, click on **Packets From Network**. This is the default setting. To view packets from a disk file, click on **Packets From File**, then click on **OK**. The Load File box appears, as shown in Figure 4-22.

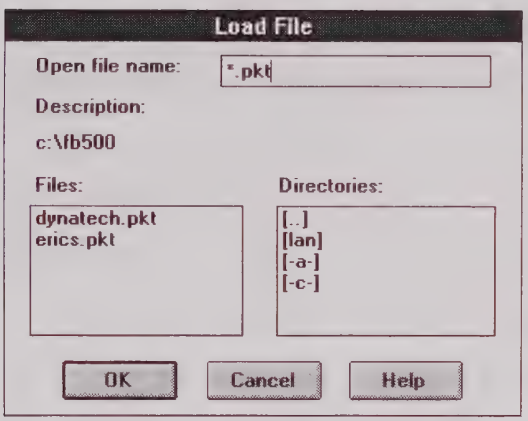


Figure 4-22
Load File Box

You may type in the full path and filename in **Open file name** or click on the appropriate directory (and subdirectory as necessary) and filename in the **Directories** and **Files** sections. All LAN Analyzer files containing captured packets have the `.pkt` extension. Click on **OK** to confirm your file selection and return to the New View Configuration window.

From the New View window, you may enter a descriptive title for your display in **View Title**. This will appear in the banner across the top of the display. **Upload Size** is how many bytes of each packet the analyzer reads at one time. The allowable range varies between token ring and ethernet analyzers. If you specify an upload size of more than 400 bytes, the analyzer retrieves the bytes in 400-byte chunks from the probe. Values below 400 means it reads packets faster, although for larger packets this may mean the whole packet is not decoded. Click on **OK** to begin displaying the captured packets.

4.7.16 The Capture Display

The packets are decoded before you see them on the display screen. The LAN Analyzer decodes the following protocols.

TCP/IP	including IP, ICMP, UDP, TCP, ARP, SNAP, TELNET, FTP, SMTP, TFTP, BOOTP, NFS, RIP, SNMP, DOMAIN, DNS, lpr, rsh, rlogin, rexec, and rwho.
DEC	including DECnet, MOP, RLP, NSP, SCP, DAP, NVTP, NICE, LAT, and CTERM.
Novell Netware	including IPX, SAP, and NCP.
AppleTalk	LLAP, ELAP, ASP, DDP, AARP, RTMP, AEP, NBP, ATP, PAP, AFP, ADSP, ZIP.
Xerox	XNS, RIP, IDP, ERROR, ECHO, SPP.
ISO	LLC1-2, CONS, CLNS, ES-IS, ISO 8073 (TP Class 0 - 4).
IBM	LLC, SNA/NETBIOS, SMB, NBP, NETBIOS, SNA/LLC, NETBEUI.
Banyan Vines	IP, RTP, ARP, ICP, IPC, SPP, SNAP, SSP.

If the LAN Analyzer cannot interpret a packet's contents using any of the protocol decodes listed above, it will display all of the packet's fields as hexadecimal bytes. The display window is shown in Figure 4-23.

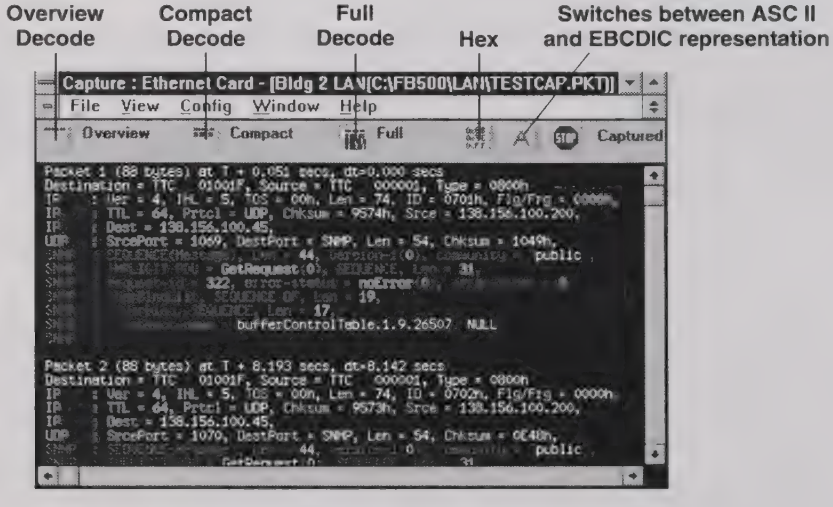

Overview Decode
Compact Decode
Full Decode
Hex
Switches between ASC II and EBCDIC representation
Capture : Ethernet Card - [Bldg 2 LAN\C:\FB500\LAN\TESTCAP.PKT]
File View Config Window Help
Overview
Compact
Full
Captured
Packet 1 (88 bytes) at T + 0.051 secs, dt=0.000 secs
Destination = TTC 01001F, Source = TTC 000001, Type = 0800h
IP : Ver = 4, IHL = 5, TOS = 00h, Len = 74, ID = 0701h, Flg/Frg = 0000h,
IP : TTL = 64, Prtcl = UDP, Chksum = 9574h, Srce = 138.156.100.200,
IP : Dest = 138.156.100.45,
UDP : SrcePort = 1069, DestPort = SNMP, Len = 54, Chksum = 1049h,
public
GetRequest
bufferControlTable.1.9.26507 NULL
Packet 2 (88 bytes) at T + 8.193 secs, dt=8.142 secs
Destination = TTC 01001F, Source = TTC 000001, Type = 0800h
IP : Ver = 4, IHL = 5, TOS = 00h, Len = 74, ID = 0702h, Flg/Frg = 0000h,
IP : TTL = 64, Prtcl = UDP, Chksum = 9573h, Srce = 138.156.100.200,
IP : Dest = 138.156.100.45,
UDP : SrcePort = 1070, DestPort = SNMP, Len = 54, Chksum = 0E40h,
public

Figure 4-23
Decoded Packet Display

You may want to set up the packet display to represent all packet fields as hexadecimal bytes. To do this, click on the **Hex** button in the display's Toolbar. The **Overview**, **Compact**, and **Full** icons determine the level of detail of the packet. **Overview** presents each packet's Source and Destination names and addresses, with a line summarizing the highest level of the protocol. **Compact** format presents the most useful fields in each protocol layer. **Full** format displays every field in the packet, and you may need to click the scroll bar on the right of your screen to view all of it.

4.8 USING SEGMENT HISTORY

Use the Segment History Task to take a snapshot of activity happening over a particular time interval, and on a particular segment of your network.

4.8.1 Setting Up a Segment History View

After you have accessed the Segment History Task, the Segment History View Setup window appears as shown in Figure 4-29.

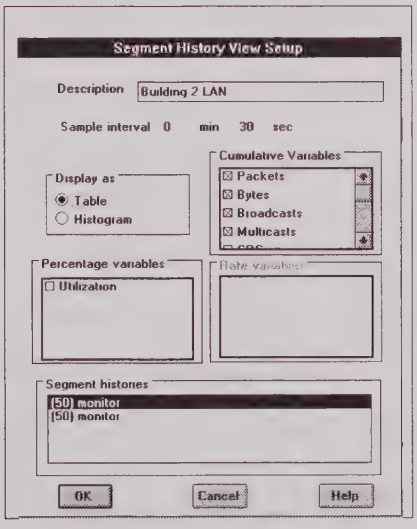


Figure 4-24
Segment History View Setup

The choices in this window are:

Description — Give a descriptive name to the view that you want to set up. Use up to 33 characters.

The sample interval is set in Configure mode to be between 1 second and 3600 seconds (1 hour) inclusive. If the sample interval chosen is outside the defined limits, a warning message appears.

Display As — Choose to display the segment history in histogram or table format, and click on the appropriate button.

Segment histories — Select the Segment History Table you want to view by clicking on it. Each entry contains the description string of a table, preceded by the owner's IP address in brackets. Unlike the configuration dialog box, you will not be allowed to delete, add to, or change any of the entries, but you are allowed to select one to view.

When you have set up the view as you want it, click on **OK** to run the Task. The setup window will be replaced with a table or histogram data display.

4.8.2 Creating and Deleting a Segment History Display

Creating a Segment History

You can configure a new segment history by selecting **View>New View...**. The Segment History View Setup box appears again.

The **Buckets requested** box allows you to choose the number of samples (buckets) to be stored. The number of samples selected must be between 1 and 8000. The number of buckets selected is validated in the same way as the sample interval boxes, that is, when you click on **OK**.

If the analyzer decides to allocate fewer buckets than you request, the following will happen:

1. The number of buckets actually granted is indicated on the configuration dialog box.

2. A message appears indicating that the request has been denied but offering you the choice of continuing with the reduced number of buckets, or canceling the request.

3. If you decide to continue, the new entry will be created. If you decide to cancel, the cursor will return to the configuration dialog box.

Deleting a Segment History

You can delete entries by selecting the appropriate entry in the list box and clicking on **Delete**. This also applies to entries owned by other IP addresses.

4.8.3 Available Segment History Statistics

You can access various types of statistics about segments. They can be divided into Cumulative and Percentage variables. Note that Rate Variables is grayed out as they aren't applicable to Segment History.

Cumulative Variables

You can select any of the counts below for the segment history table you have selected.

These variables are counts of packets or bytes that are transmitted or received by the segment during the period being viewed. The term "byte" refers to an 8-bit entity, and means the same as the term "octet". A "packet" is an Ethernet or Token Ring frame.

The cumulative variables for **Ethernet** are:

Total packets (transmitted)	Total number of packets transmitted on a given segment.
Total bytes (transmitted)	Total number of bytes transmitted on a given segment.
Broadcasts	Total number of broadcast packets transmitted on a given segment.
Multicasts	Total number of multicast packets transmitted on a given segment.
Dropped packets	Total number of events in which packets were dropped due to a lack of resources. This number isn't necessarily the number of dropped packets; it is the number of times that the condition was detected.
CRC Alignment Errors	Ethernet packets with a length between 64 and 1518 bytes, excluding the frame bits but including the FCS, and are not an integral number of bytes or have an invalid FCS.
Short packets	Packets less than 64 bytes in length, excluding the framing bits but including the FCS. These packets are well-formed otherwise.

Long packets	Ethernet packets longer than 1,518 bytes, excluding the framing bits but including the FCS. These packets are well-formed otherwise.
Fragments	Packets which are not an integral number of bytes in length or have a bad FCS. These packets are all less than 64 bytes long, excluding the framing bits but including the FCS.
Jabbers	Ethernet packets longer than 1,518 bytes, excluding the framing bits but including the FCS bytes. These packets all have either a non-integral number of bytes or a bad FCS.
Collisions	The number of collisions on this Ethernet segment.

The cumulative variables for **Token Ring** are:

Total packets (transmitted)	Total number of packets transmitted on a given segment.
Total bytes (transmitted)	Total number of bytes transmitted on a given segment.
Broadcasts	Total number of broadcast packets transmitted on a given segment.
Multicast	Total number of multicast packets transmitted on a given segment.
Dropped packets	The total number of events in which packets were dropped due to a lack of resources. This number isn't necessarily the number of dropped packets; it is the number of times that the condition was detected.
MAC packets	The total number of MAC packets (excluding packets with errors) transmitted.
MAC bytes	The total number of octets of data in MAC packets (excluding those in packets with FCS errors) transmitted on the network (excluding framing bits, but including FCS octets).
Purge events	The total number of times that the ring enters the ring purge state from normal ring state. The ring purge state that comes in response to the monitor contention or beacon state is not counted.
Purge packets	The total number of ring purge MAC packets detected.
Beacon events	The total number of times that the ring enters a beaconing state (beaconFrame StreamingState, beaconBitStreamingState, or beaconSet Recovery Mode State). A change of the source address of the beacon packet does not constitute a new beacon event.

Beacon packets	The total number of beacon MAC packets detected.
Contention events	The total number of times that the ring enters the monitor contention state from normal ring state or ring purge state. The monitor contention state that comes in response to a beacon state is not counted.
Claim tokens	The total number of claim token MAC packets detected.
NAUN changes	The total number of NAUN changes detected.
Line errors	The total number of line errors reported in error reporting packets detected.
Internal errors	The total number of adapter internal errors reported in error reporting packets detected.
Burst errors	The total number of burst errors reported in error reporting packets detected.
AC errors	The total number of Address Copied (AC) errors reported in error reporting packets detected.
Abort errors	The total number of abort delimiters reported in error reporting packets detected.
Lost Frame errors	The total number of lost frame errors reported in error reporting packets detected.
Congestion errors	The total number of receive congestion errors reported in error reporting packets detected.
FC errors	The total number of Frame Copied errors reported in error reporting packets detected.
Frequency errors	The total number of frequency errors reported in error reporting packets detected.
Token errors	The total number of token errors reported in error reporting packets detected.
Error reports	The total number of soft error report frames detected.
Poll events	The total number of ring poll events detected (i.e., the number of ring polls initiated by the active monitor that were detected).
Active stations	The total number of stations participating in the ring poll.

Percentage Variables

Utilization	Is the percentage of **Ethernet** network bandwidth used in the period of the selected segment history, including error packets.

NOTE: There are no percentage variables available for Token Ring networks.

4.9 USING TRAFFIC GENERATION

Use the Traffic Generation Task to:

- Capture data and configure the analyzer to generate traffic using data specified by the user, or from the analyzer's capture buffer
- Start the analyzer generating traffic
- View the load being generated, the number of packets, collisions and deferred transmissions.

4.9.1 Configuring Generation

After you have accessed Traffic Generation, the Traffic Generation Config window appears as shown in Figure 4-25.

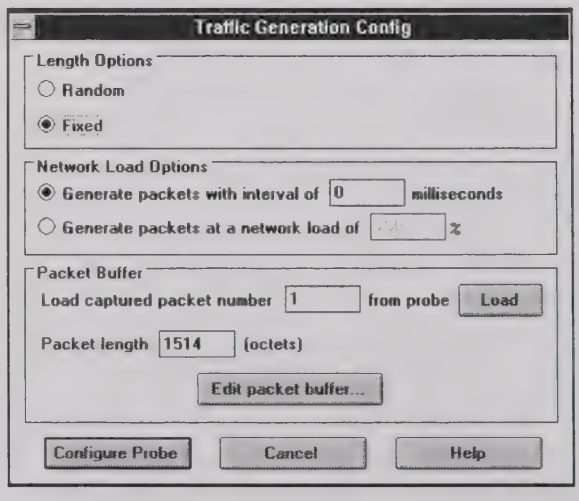


Figure 4-25
Traffic Generation Config

The configurable choices here are:

Length Options — Causes a random or fixed-length packet to be generated.

Network Load Options — There are two methods of selecting the load to be generated on the network:

If you want to define the generated load by the interval between packets generated, select **Generate packets with an interval of ??? milliseconds**. Then enter the interval desired.

If you want to define the generated load as a percentage of the network's maximum load, select **Generate packets at a network load of ??? percent**. Then enter the percentage desired.

Packet Buffer — Enter (in the **Load captured packet number** box) the number of the packet that you want to copy from the capture buffer. Click on **Load** to retrieve the specified packet and load it into the editing buffer.

Enter a **Packet length** of between 14 and 2048 for Ethernet, between 18 and 4048 for 4 Mb/s Token Ring, or between 18 and 18000 for 16 Mb/s Token Ring. This defines the length of packet generated if **Fixed** length is selected, or the mean length if **Random** length is selected (in the **Length Options** parameter).

Edit packet buffer... — Click on **Edit packet buffer...** to open the applicable level template, and edit the packet data that is generated. The MAC Level Template is displayed for Ethernet, and the MAC and LLC Level Template is displayed for Token Ring.

Use the Templates to enter values for any of the parameters listed below. Select the Template type you want to use to change any data values and click on **Edit Template**. Parameters in this dialog box are described in the following two sections.

NOTE: The dialogs used to specify the data are the same as are used to specify filters in the Capture Task. However, buttons marked **=** next to some fields are grayed out for Traffic Generation.

You can enter a value into any **Hex** field using a binary rather than Hex input. To do this, double-click on the **Hex** field. This displays a dialog box with one Hex and one binary field. As you enter a bit pattern in the binary field, the equivalent Hex number appears in the Hex field. Click **OK** to return to the main template box, where your input will be displayed as a Hex number.

Double-click on either the **Destination**, **Source**, or **Type** fields to edit the bits, and display the Bit Level Edit box. Figure 4-26 shows the Bit Level Edit box as a number is entered.

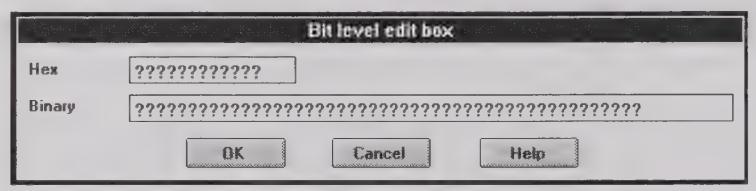


Figure 4-26
Bit Level Edit Box

If you leave one, two, or three bits within an octet as a wildcard, the Hex display shows these bits as a dollar sign (**$**) rather than a question mark.

4.9.2 The MAC Level Dialog for Ethernet

To set up the data in the packets you want to generate, click on **Edit packet buffer...**. The MAC Level Template appears. The Ethernet MAC Level Template is shown in Figure 4-27.

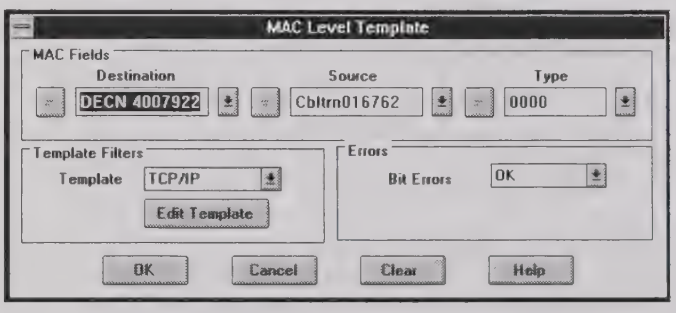


Figure 4-27
Ethernet MAC Level Template

Choices in this template are:

Destination Specifies the station(s) the generated data is being sent to.

Source Specifies the station(s) where the generated data is being sent from.

Click on the arrow to display the list of stations that the analyzer can "see". To select a station, click on its name or address. If you do not want to select one station or a subset of stations, choose **All Stations** in the dialog box.

Type

Every Ethernet packet has a 2-byte **Type** field that the Ethernet driver at the packet's destination address uses to direct the packet up to the appropriate protocol module. If you are using the Hex template you can select any of these packet types, or specify your own by typing in hexadecimal characters.

TCP/IP	Transmission Control Protocol/Internet Protocol
ARP	Address Resolution Protocol
AARP	Apple Address Resolution Protocol
APPLETALK	Apple Computer's Ethernet
NETWARE1	Novell's NetWare 1
NETWARE2	Novell's NetWare 2
MOP1	Maintenance Oriented Protocol 1
MOP2	Maintenance Oriented Protocol 2
DECNET	Digital Equipment Network
LAT	Local Area Transport Protocol
LAVC	DEC LAVC
Banyan1	Banyan VINES 1
Banyan2	Banyan VINES 2
NBP	Name Binding Protocol

Bit Errors

The **Bit Errors** field lets you generate packets containing CRC/Alignment errors:

OK Use this option only to generate packets without CRC/Alignment errors.

CRC/Align Select this option to generate packets that either have a non-integral number of bytes in length or have an invalid Frame Check Sequence.

Don't Care This option is not relevant to this version of this Task.

Use the **Clear** button to set all the fields to wildcards. (This is the equivalent of setting all the characters to zero.) Note that clicking on **Clear** also places wildcards in any fields you set in the other traffic generation templates.

When you have set the data fields, click on **OK** to return to the Traffic Generation Config window.

NOTE: Clicking on **Configure Probe** starts the generation of traffic.

4.9.3 The MAC and LLC Level Dialog for Token Ring

The Token Ring MAC and LLC Level Template is shown in Figure 4-28.

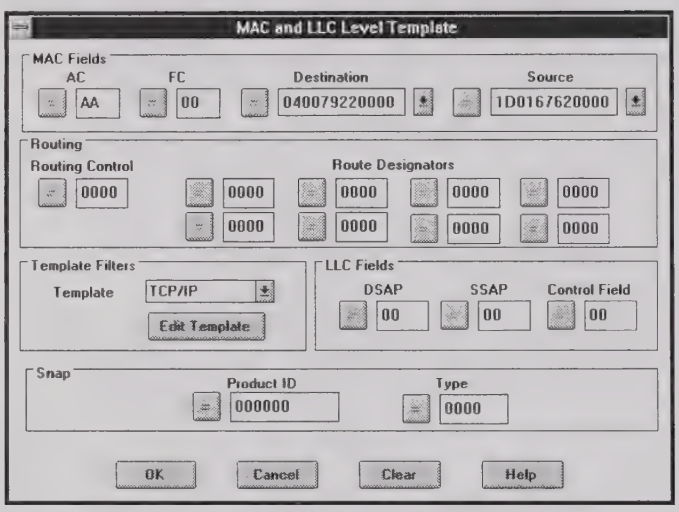


Figure 4-28
MAC and LLC Level Template

Choices in this template are:

MAC Fields

AC Access control. Although available, it is not relevant to this application.

FC Frame control. Defines the type of frame that will be generated. The first byte in **FC** determines whether it is a MAC frame or a non-MAC frame. When the first byte is a **4**, it is defined as a non-MAC frame; and when it is a **0**, it is defined as a MAC frame.

Use **Destination** and **Source** to specify which stations packets are transmitted to or from. An invalid MAC field will cause a packet not to be sent.

Routing

This section is optional. It is necessary only when packets are being generated from outside the source ring. If this is the case, enter data for the **Routing Control** field and up to eight 2-byte **Route Designators**.

LLC Fields

In the **DSAP**, **SSAP**, and **Control Field**, enter the data to define the complete LLC. The **DSAP** and **SSAP** address fields refer to the service access points that interface with the network layer and the link layer. The control field indicates that the generated packet will be one of three types: information, supervisory, or unnumbered packet.

SNAP

802.5 networks use SNAP to encapsulate Ethernet packets. Enter the **Product ID** and **Type** in the fields provided.

4.9.4 Template Filters

Once you have set the variables in the MAC and LLC Level dialog box, you can specify the contents of the data fields.

You can view these fields in a number of ways, depending on the protocol you want to use, or you can use Hex. Select the **Template** you want from the list and click on **Edit Template**.

If you select TCP/IP in the **Template** field, the TCP Filter Template appears as shown in Figure 4-29.

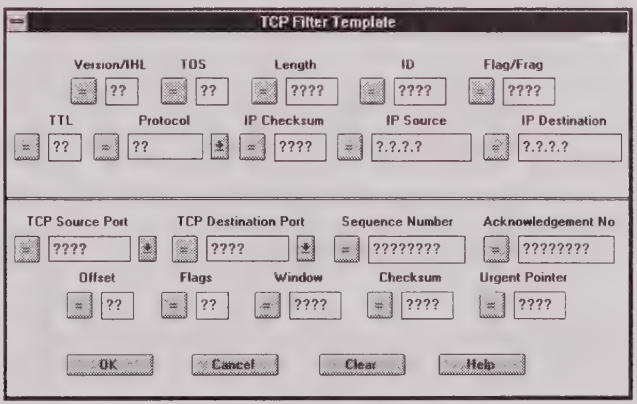


Figure 4-29
TCP Filter Template

Edit these filter fields as necessary. To select a field, click on it. An arrow box indicates a hidden list of values; click on the arrow to display the list. Change the value of a field by overwriting the current value or by selecting a value from the pulldown list.

NOTE: As with the MAC Level Template dialog box, you can enter values in binary rather than in Hex. Do this by double-clicking on the appropriate dialog box.

Click on **Clear** to set all the fields to wildcards, which in this application is the equivalent of setting all the characters to zero. Note that clicking on **Clear** also places wildcards in any fields you set in the other traffic generation templates.

When you have set the data fields you want, click on **OK** to return to the MAC and LLC Level dialog. Click **OK** to return to the Traffic Generation Config window.

NOTE: Clicking on **Configure Probe** starts the generation of traffic.

4.9.5 Displaying Traffic Generation

Traffic Generation is restarted and a new view window is created every time you click on **GO**. The view is updated every second; this parameter is not user-configurable. The title of each view is the date and time when the traffic generation was started.

It is possible to only view one active Traffic Generation display at a time. All inactive Traffic Generation views will be titled with Inactive followed by the time traffic generation started. Note that Ethernet and Token Ring displays are different, as shown in Figures 4-30 and 4-31.

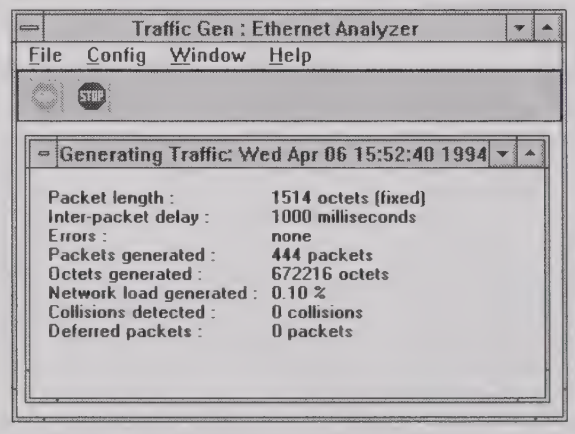

Traffic Gen : Ethernet Analyzer
File Config Window Help
STOP
Generating Traffic: Wed Apr 06 15:52:40 1994
Packet length : 1514 octets (fixed)
Inter-packet delay : 1000 milliseconds
Errors : none
Packets generated : 444 packets
Octets generated : 672216 octets
Network load generated : 0.10 %
Collisions detected : 0 collisions
Deferred packets : 0 packets

Figure 4-30
Ethernet Traffic Generation Display

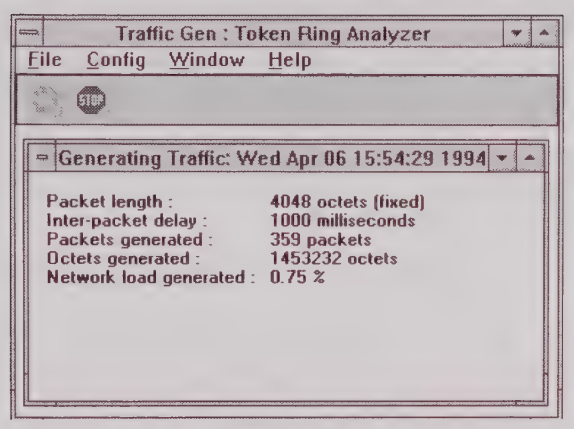

Traffic Gen : Token Ring Analyzer
File Config Window Help
Generating Traffic: Wed Apr 06 15:54:29 1994
Packet length : 4048 octets (fixed)
Inter-packet delay : 1000 milliseconds
Packets generated : 359 packets
Octets generated : 1453232 octets
Network load generated : 0.75 %

Figure 4-31
Token Ring Traffic Generation Display

To halt traffic generation, click on **STOP**. To re-activate, click on **GO**.

Note that the LAN Analyzer can only generate one set of traffic at a time.

4.9.6 General Traffic Generation Stoppage

Once Traffic Generation is restarted, there are a number of events that will cause it to halt. The following list of messages indicates the message that is displayed and a brief explanation of what may have caused the message to be displayed. Clicking on **OK** clears the message from the screen.

"Traffic generation halted due to another user configuring the Probe for traffic generation." — Another manager has reconfigured traffic generation.

"Traffic generation halted due to an application timeout error." — The manager has not read the traffic generation results within a time period. The current time period is 30 seconds.

"Traffic generation halted due to an unknown error." — An unspecified error occurred.

4.9.7 Ethernet Traffic Generation Stoppage

Once Traffic Generation is restarted for Ethernet, there are a number of events that will cause it to halt. The following list of messages indicates the message that is displayed and a brief explanation of what may have caused the message to be displayed. Clicking on **OK** clears the message from the screen.

"Traffic generation halted due to loss of Carrier Sense signal." — No Carrier Sense signal between beginning of Destination Address and end of Frame Check Sequence."

"Traffic generation halted due to loss of Clear to Send signal." — Transmission unsuccessful due to loss of Clear-to-Send signal.

"Traffic generation halted due to a Probe DMA underrun error." — DMA underrun error on Ethernet Coprocessor.

"Traffic generation halted due to an inter frame heart beat error." — During the Interframe Spacing period after the previous transmission, a pulse was detected on the Collision Detect pin.

"Traffic generation halted due to too many collisions." — Excess collisions generated in an attempt to transmit one frame.

4.9.8 Token Ring Traffic Generation Stoppage

Once Traffic Generation is restarted for Token Ring, there are a number of events that will cause it to halt. The following list of messages indicates the message that is displayed and a brief explanation of what may have caused the message to be displayed. Clicking on **OK** clears the message from the screen.

"Traffic generation halted due to transmission of an unenabled MAC frame. Check the Source Class and PFC ATTN field of the generated frame." — The frame to be transmitted was defined as a MAC frame with the source class as zero or with the PFC ATTN field greater than one.

"Traffic generation halted due to transmission of an illegal frame. Check FC value of the generated frame." — The frame to be transmitted has its Most Significant Bit in the FC field set to one.

"Traffic generation halted due to adapter closed." — The adapter has closed and traffic generation can not continue.

4.10 USING THE TEST APPLICATION

Use the Test Application Task to perform packet echo and forwarding tests on selected segments.

The packet tests involve a second node. The packet tests are **ISO**, **XNS** (Ethernet only), **Xerox Echo** (Ethernet only), **Xerox Loop** (Ethernet only), and **Tx-Forward** (Token Ring only). You can perform packet tests on only one station

at a time. If you want to perform tests on many stations, you must start tests on one station, get the results, and then set up a test for the next station. For this reason, the Test Application does not have the conventional configuration dialog box or a view dialog box.

Views are built up dynamically as the tests are running. Since the analyzer performs a set of tests on one station at a time, once the results for a station have been added to the view, the next test will start and the previous results will be overwritten. The view is a historical view of what is discovered; it is not a view of stored data.

4.10.1 Setting Up the Test Application

Once you have accessed the Test Application Task, the Test Mode Configuration box appears, as shown in Figure 4-32.

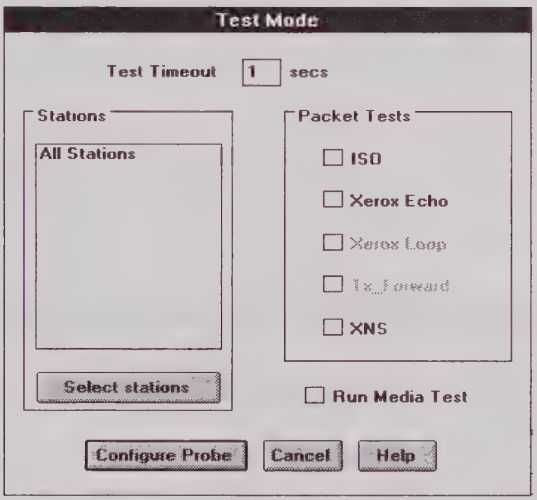


Figure 4-32
Test Mode Configuration Box

The configurable choices in this box are:

Test Timeout — Enter a value from 1 to 10 seconds. This is the maximum time the analyzer will wait for a test packet to return. The value entered will be validated when you click on **Configure Probe**. If the value is outside this range, a warning message appears and the tests are not run. Enter a valid timeout period and **Configure Probe** again.

Packet Tests

Check the boxes of the tests you want to run. If a box is checked, this test will be applied to all of the selected stations.

The Xerox Loop test is only available if the **Xerox Echo** box is checked. This is because the Xerox Loop test is only run between stations passing the Xerox Echo test.

The **Tx_Forward** box only applies to the Token Ring Analyzer, so it will be grayed out for the Ethernet Analyzer. Similarly, the Xerox and XNS tests only apply to the Ethernet Analyzer, and will be grayed out for the Token Ring Analyzer.

Run Media Test

The **Run Media Test** selection allows testing of the attached media. The Ethernet test performs both a Time Domain Reflectometry (TDR) and transceiver heartbeat (SQE) test. TDR tests are used to detect the distance of open circuits or shorted circuits on the network cable. SQE tests check on the collision detect interface in the transceiver.

The Token Ring test shows the results from the last time the test instrument attempted to open the ring.

Stations

The **Stations** section contains a list of all the hosts that you may perform the tests on. If you entered the Test Application with **All Stations** selected, **All Stations** should appear in this section now. If you want to select a specific subset of All Stations, click on **Select stations** to bring up the Select Stations box, shown in Figure 4-33.

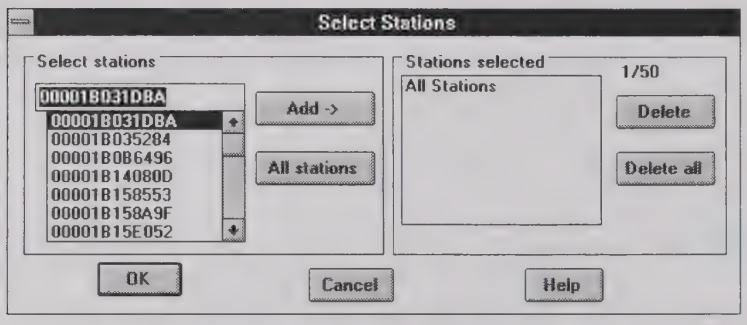


Figure 4-33
Select Stations

In this dialog box, the **Select stations** section shows a list of all available stations; you can scroll through this list and highlight as many stations as required.

To select a station, click to highlight it, and then click on **Add**. You will see that station appear in the **Stations selected** section. Do this for each station you want to use. If you want to test every station, click on **All Stations**; then **All Stations** appears as the only entry in the **Stations selected** list. Click on **Cancel** to cancel any changes to your selection since the previous test. Once you have set the parameters, click on **Configure Probe**. This takes you to the main Test Application window.

Click on **GO** on the Toolbar to start the selected tests. At this point **STOP** becomes available to abort the tests before they are complete.

The results of the tests now appear in a newly created view window as they arrive, as shown in Figure 4-34.

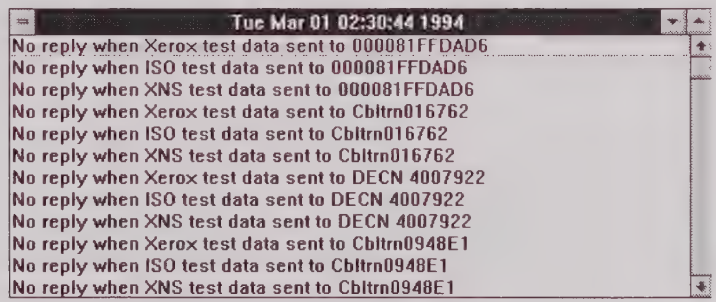

Tue Mar 01 02:30:44 1994
No reply when Xerox test data sent to 000081FFDAD6
No reply when ISO test data sent to 000081FFDAD6
No reply when XNS test data sent to 000081FFDAD6
No reply when Xerox test data sent to CbItrn016762
No reply when ISO test data sent to CbItrn016762
No reply when XNS test data sent to CbItrn016762
No reply when Xerox test data sent to DECN 4007922
No reply when ISO test data sent to DECN 4007922
No reply when XNS test data sent to DECN 4007922
No reply when Xerox test data sent to CbItrn0948E1
No reply when ISO test data sent to CbItrn0948E1
No reply when XNS test data sent to CbItrn0948E1

Figure 4-34
Test Results in New View Window

4.11 USING RING STATS

Use the Ring Stats Task to collect and display statistics about the packets transmitted and received by active hosts on your Token Ring network. Note that Ring Stats is a Token Ring Task, so this section only applies to the FIREBERD 383/583 Token Ring LAN Analyzer.

4.11.1 Setting Up a Ring Stats View

Once you have accessed the Ring Statistics Task, the Statistics View Setup window appears, as shown in Figure 4-35.

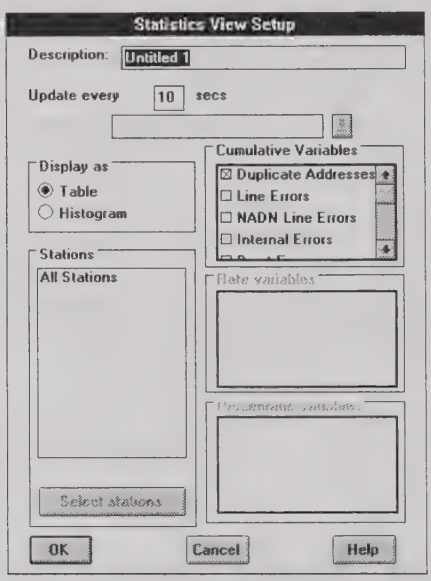


Figure 4-35
Ring Station Statistics View Setup

The choices in this window are:

Description — Enter a descriptive name for the view you are setting up; use up to 39 characters.

Update every — Determines how often the data in your display will be replaced with new data. Enter a value between 1 and 99 (seconds).

Order by — Order the display according to the value of any variable in this pull-down list, if you have selected some but not all hosts as your data sources. If you have selected **All Stations** as your data source, this field is grayed out and the data will be displayed according to the order it appeared on the ring.

Display as — Display the statistics data as a table or as a histogram by clicking on the button beside your choice.

Stations — **All Stations** is the default setting.

Selecting Variables

The remaining sections in the Statistics View Setup window show categories of variables: Cumulative, Rate and Percentage. Only Cumulative variables are applicable here. To select a variable, click on its check box.

When all the setup parameters are as you want them, click on **OK** to begin running the Ring Stats Task. The setup window will be replaced by a histogram or table of the variables you have selected.

4.11.2 Ring Stats Cumulative Variables

You may select any of the counts below for the host(s) you have selected.

Line Errors	The total number of adapter internal errors reported by this station in error reporting packets.
Burst Errors	The total number of burst errors reported by this station in error reporting packets.
Address Copied	The total number of AC errors reported by this station in error reporting packets detected.
Abort Delimiters	The total number of abort delimiters reported by this station in error reporting packets.
Lost Frames	The total number of lost frame errors reported by this station in error reporting packets.
Congestion	The total number of receive congestion errors reported by this station in error reporting packets.
Frame Copied	The total number of FC errors reported by this station in error reporting packets.
Frequency	The total number of frequency errors reported by this station in error reporting packets.
Token Error	The total number of token errors reported by this station in error reporting packets.
Beacon Frames	The total number of beacon frames reported by this station in error reporting packets.
NADN Beacons	The total number of beacon frames detected by the analyzer that name this station as the nearest active upstream neighbor.
Insertions	The number of times the analyzer detected this station inserting onto the ring.
NADN Line Errors	The total number of line errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the analyzer.
Duplicate Addresses	The number of times this station experienced a duplicate address error.

NADN Burst Errors	The total number of burst errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the analyzer.
Internal Errors	The total number of line errors reported in error reporting packets sent by the nearest active downstream neighbor of this station and detected by the analyzer.

4.12 USING THE ERROR

Use the Error Task to collect and display selected error packets transmitted and received by hosts on a Token Ring network. Note that Error is a Token Ring Task, so this section only applies to the FIREBERD 383/583 Token Ring LAN Analyzer.

4.12.1 Setting Up an Error View

After you have accessed the Error Task, the Config Error box appears, as shown in Figure 4-36.

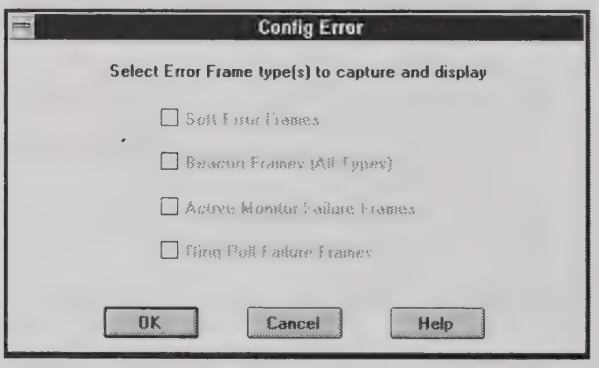


Figure 4-36
Config Error

The four error packet types that can be captured are:

Soft Error Frames	Monitors errors that the Token Ring system software is handling. Errors are classified as soft errors if they are intermittent.
Beacon Frames (All Types)	Monitors hard errors. Errors are classified as hard errors if they disrupt the operation of the network.

Active Monitor Failure Frames	Monitors errors of the active monitor.
Ring Poll Failure Frames	Monitors failures in the normal procedure of neighboring stations notifying each other of their presence.

Click on the check box(es) of the error(s) that you want to capture and view, then click on **OK** to confirm your selection.

To set up a new view, select **View>New View**. A display like the one in Figure 4-37 appears. There is no Edit View option because there are no user-configurable parameters for View.

Figure 4-37
New View

When the new view is created, the complete contents of the error packet table will be displayed on the screen. Packets are decoded and added to the bottom of the display; every 10 seconds, new error packets are retrieved and added to the display.

If the analyzer allocates a very small packet table or if the arrival rate of packets is greater than 100 every 10 seconds, then some packets will be overwritten before the analyzer has captured and displayed them. In this unlikely event, the gap will be indicated by an entry in the view stating:

```
**** n error packets missed ****
```

where **n** is the number of packets missed.

Use the scroll bar to access the non-visible parts of the view. Each packet has its time of capture displayed, in relation to the FIREBERD 300/500's internal clock. To stop the window from scrolling, select **View>Freeze View**. This enables you to look at a particular error before it is "scrolled off" the screen. Note that errors are still collected while this activity is in progress.

Saving Error Files to Disk

To save an error file to disk, first select the window you want to save. Then, pull down **File>Save or File>Save As**. You will be shown the **Save File** box where you can specify a filename and a directory path. The filename you specify will be given the **.txt** extension by default. A straight ASCII copy of the contents of a view will be saved to a file.

4.13 USING PROTOCOL STATS

Use the Protocol Stats Task to collect and display selected statistics about protocol statistics transmitted and received by hosts on your network.

4.13.1 Setting Up a Protocol Stats View

After you have accessed the Protocol Statistics Task, the Statistics View Setup window appears, as shown in Figure 4-38.

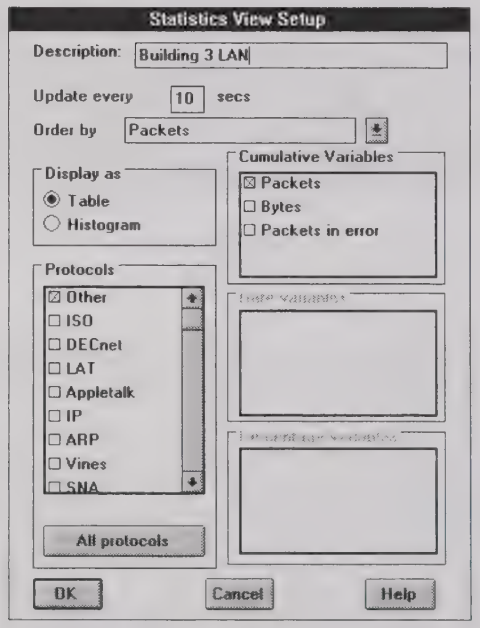


Figure 4-38
Protocol Statistics View Setup Window

The choices in this window are:

Description Enter a descriptive name for the view you are setting up; use up to 39 characters.

Update every Determines how often the data in your display will be replaced with new data. Enter a value between 1 and 99 (seconds).

Order by A pull-down list of ordering options that sorts the data you collect.

Display as Display the statistics data as a table or as a histogram by clicking on the button beside your choice.

Protocols List all the protocols about which you want to collect data. Click on the check box of each protocol you want to select. The **Other** check box allows you to select any protocol which is not specifically mentioned in the list box.

All protocols Click on this button to select all the protocols for the view.

When all of your test parameters are as you want them, click on **OK** to begin running Protocol Stats. The Protocol Stats window is replaced by a histogram or table of the variables you have selected.

4.13.2 Available Protocol Statistics

This section describes the Cumulative variables available in the **View Setup** window. You can access these variables by clicking on the relevant check box. The Rate and Percentage variables are not available with this Task, and are therefore grayed out.

Cumulative Variables

You can select any of the counts below for the protocols you have selected.

Packets and Bytes Counts of the number of either packets or bytes that are transmitted or received using the protocols you have selected. A packet is an Ethernet or Token Ring frame.

Packets in error Any non-valid packet as defined by Ethernet or Token Ring specifications.

4.14 DISPLAYING AND PRINTING INFORMATION

You can tailor the way the Tasks display information to suit your needs. You can display information as tables or histograms, and have multiple displays running at once. This section uses Segment History as an example of how to display information, describes the various display options available to you, demonstrates the ways you can represent the data you have collected, and describes saving and printing the data you display.

4.14.1 Displaying Results as Tables

Tables are presentations of test results using numbers and text. Your test results from the Tasks can be represented in table format, as shown in Figure 4-39.

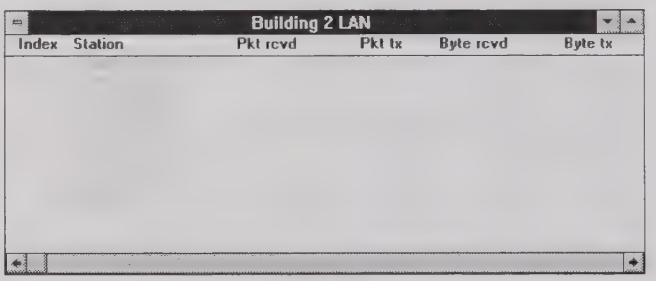


Figure 4-39
Example of a Table Display

Each variable you selected when you set up the view will appear as a column header in the display. You can use the scroll bar on the right side of the display to scroll up and down through the table, and you can change the size of the display box to suit your needs. If the table is wider than the display window, use the horizontal scroll bar that appears across the bottom of the display to scroll through table left and right.

4.14.2 Displaying Results as Histograms

Histograms are bar-graph representations of test results. Test results from the Tasks can be represented in histogram format, as shown in Figure 4-40.

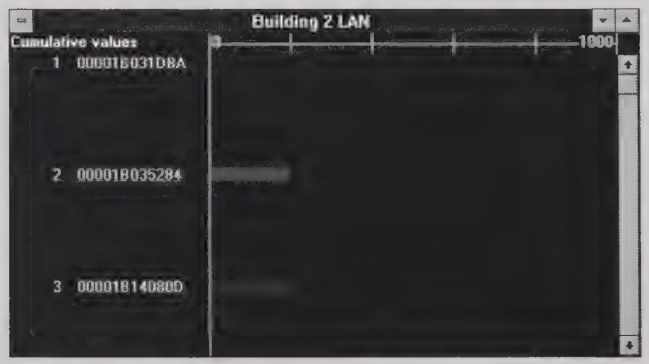


Figure 4-40
Example of a Histogram Display

There are three types of variables:

Cumulative	Counts of packets, bytes, or error packets (labeled **C** on the Histogram Display).
Rate	The number of packets of a given type per second sent by a host (labeled **R** on the Histogram Display).
Percentage	The percentage of bandwidth used by packets to or from a host (labeled **P** on the Histogram Display).

Select any combination of variables from these three types. The LAN Analyzer displays a separate histogram for each variable type. Variables of the same type will be represented on the same histogram, with differently colored bars for each variable. For example, if you selected Packets received and Bytes transmitted (both cumulative variables) and Receive rate (a rate variable), the display shows one graph for both Packets received and Bytes transmitted, and one for Receive rate. Use the **C**, **R**, and **P** buttons in the Toolbar to switch to a histogram representing another type of variable.

The Toolbar also has a **Key** icon. When you click on it, the histogram key appears, explaining which variable each color represents. If the key is displayed in an inconvenient place, click on its title bar and drag it to a more convenient location.

You can change the scale of the histogram bars to suit your display space. Since cumulative variables tend to have very high values, there are special scales for them. From the Toolbar, pull down the menu under the histogram button labeled **C**. Select an appropriate scale for your data. There are also scaling buttons for percentage variables (labeled **P**) and for rate variables (labeled **R**). You can switch from histogram to table format without having to go back to the setup window. Click on the **Table** icon in the menu bar.

You can display several views simultaneously in separate windows. To set up a new view, pull down **View>New** from the menu bar; this allows you to create a new display without closing the current view. The displays do not need to be of the same type. For example, you could display a table of error types in one window while displaying a histogram of packet lengths in another. When the new view is displayed, you can arrange the two views by pulling down **Window** and selecting either **Tile** or **Cascade** to arrange the histograms. Once you display a view, if you want to change it in some way, pull down **View>Edit View** to make the changes to its setup.

4.14.3 Saving and Printing Data

Saving Data

Data displayed on the screen can be saved to the FIREBERD 300/500's hard drive or a floppy disk by pulling down **File>Save** or **File>Save As** and giving the file a name. These are ASCII files, suitable for importing into spreadsheet programs such as Lotus 1-2-3 or Microsoft Excel.

Printing Data

The data can also be printed. Refer to the Test Manager On-Line Help or the *FIREBERD 300/500 Internetwork Analyzer User's Guide* for more information about printing files.

Printing Captured Packets

The procedure for printing captured packets is different from printing test files. To print captured packets, do the following:

1. With the captured packets on your screen, press **<PrtSc>**. This copies the screen onto the Windows Clipboard.

2. Cut and paste the captured packets into another application, such as a spreadsheet.

SECTION 5
EVENTS, CUSTOM GRAPHING, AND LOGGING

5.1 SECTION SUMMARY

This section describes the Event functions of LAN Analyzer. These include the Event Browser, Event Log, the Graph Data and Log Data tasks, and the Address Translation Table. Additionally, this section describes remote operations with the Telnet application.

5.2 EVENTS AND THE EVENT BROWSER

Events indicate when something significant happens on the network. The Event icon (a bell) is always displayed, but may be hidden in the background. When an event occurs, the Event icon rises to the foreground of the screen.

If the Event icon is white, this shows that there are no unacknowledged events, or that all events have priority "None". To acknowledge an event, double-click on the Event icon, and pull down the **Acknowledge** menu.

Events are generated in two ways:

- The node informs the analyzer of a change in its state (e.g., **Link Down**, **Cold Start**), or an occurrence (**Management Session Started**). This is done using the SNMP trap mechanism. All standard SNMP traps are reported. The analyzer is set up to watch for alarms. When the analyzer detects that an alarm has occurred, it sends out a SNMP trap. You can then find out what triggered the trap by using the Event Browser to look through the Event log.

- You ask the analyzer to check for a change in the state of a node (e.g., **Graph Parameter** or **Threshold Exceeded**).

You can view events using the Event Browser, and log these Events to a file.

5.2.1 Event Priority and Parameters

An event has the following parameters:

Priority — Priority of event. An event has one of the following priorities:
- Critical (the highest priority)
- Warning
- Informational
- Unknown
- No status

Node	Name of the node that you assigned to it in **Analyzer>Describe...**.
Event	Type of event that occurred, such as **Node Dead**.
Node Class	Type of analyzer card, such as **Ethernet Analyzer** or **Token Ring Analyzer**.
Time	Time that the LAN Analyzer logged the event.
Acknowledged	An **X** indicates that the event is acknowledged.
Note	Your notes. Click twice on the entry to bring up a notepad. An **X** in the Note column indicates a note exists.

5.2.2 Acknowledging Events

When an Information event occurs, double-click on the Event icon and pull down the **Acknowledge** menu. This brings up the Event Browser and acknowledges the event. All unacknowledged events are automatically acknowledged when you exit the LAN Analyzer, but all acknowledged events survive until you delete the file.

5.2.3 Event Types

The following is the list of events, but doesn't include traps, which are all informational.

MIB Traps

Cold Start	OK
Warm Start	OK
Link Down	Warning
Link Up	OK
Authentication Failure	Info
EGP Neighbor Loss	Info
Transmission Timeout	Info

Graphing/Logging

Graph Threshold Exceeded	Info
Within Graph Threshold	Info
Log Threshold Exceeded	Info
Within Log Threshold	Info

5.2.4 The Event Browser

The Event Browser enables you to read and manipulate the Event log. The Event icon shows when an event is outstanding (unacknowledged). You have to enter the Event Browser to acknowledge an event. To enter the Event Browser, double-click on the Event icon. Figure 5-1 shows the Event Browser display.

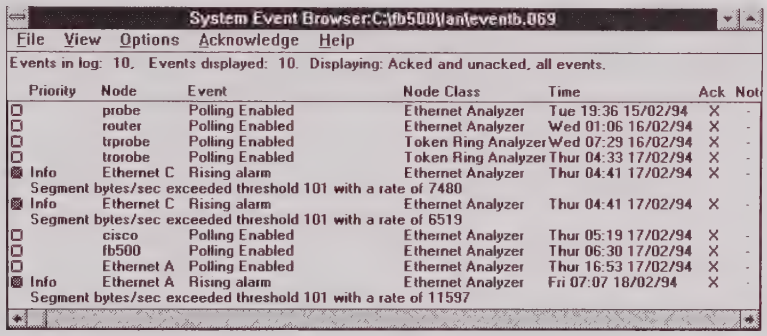

System Event Browser:C:\fb500\lan\eventb.069
File View Options Acknowledge Help
Events in log: 10. Events displayed: 10. Displaying: Acked and unacked, all events.
Priority Node Event Node Class Time Ack Not
probe Polling Enabled Ethernet Analyzer Tue 19:36 15/02/94 X -
router Polling Enabled Ethernet Analyzer Wed 01:06 16/02/94 X -
trprobe Polling Enabled Token Ring Analyzer Wed 07:29 16/02/94 X -
trprobe Polling Enabled Token Ring Analyzer Thur 04:33 17/02/94 X -
Info Ethernet C Rising alarm Ethernet Analyzer Thur 04:41 17/02/94 X -
Segment bytes/sec exceeded threshold 101 with a rate of 7480
Info Ethernet C Rising alarm Ethernet Analyzer Thur 04:41 17/02/94 X -
Segment bytes/sec exceeded threshold 101 with a rate of 6519
cisco Polling Enabled Ethernet Analyzer Thur 05:19 17/02/94 X -
fb500 Polling Enabled Ethernet Analyzer Thur 06:30 17/02/94 X -
Ethernet A Polling Enabled Ethernet Analyzer Thur 16:53 17/02/94 X -
Info Ethernet A Rising alarm Ethernet Analyzer Fri 07:07 18/02/94 X -
Segment bytes/sec exceeded threshold 101 with a rate of 11597

Figure 5-1
Event Browser Display

You can filter events before viewing them. This can be done by: priority, device class, node name, event type, or time (from and to, allowing an interval to be examined). Double-click on the event listed for a Notepad search string. You can save filtered events to a file, and apply filters to acknowledged events.

Features of the Event Browser display are:

Color — A color next to the event shows its priority.

Priority — The event status in words — critical, warning, and so on.

Node — The first ten characters of the name given in the **Describe** box.

Event — Event type.

Node class — The device type.

Time — The time when the event occurred.

Ack — A "—" shows this event is unacknowledged. When you display all events, an **X** marks acknowledged events.

Note — An **X** in this column shows there is Notepad information on this event. Double-click on the event line to display this user-written information.

The **View>Unacknowledged Events** menu option is enabled when you enter the Event Browser. This shows you all the events you have not responded to (unacknowledged events). When it is first initialized, the Event Browser shows only unacknowledged events. Some events are associated with a text message. This is printed under the event line, when **View>Show Info Messages** is enabled. This is the default.

5.2.5 Event Browser Options

File — The two options of **File** are:

Open Log enables you to open and browse through event log files that you've previously created and stored.

Save Log has two sub-options: **Save displayed as ASCII** stores events in a text file, and **Save displayed as Log** stores events in a log to be read later. This is very useful if you want to save a subset of Events for later use.

View — Controls the events displayed. Check marks on the pull-down list show what is currently set, either **Unacknowledged Events**, **Filtered Events**, or **All Events**.

Show Info Messages displays any additional text for an event. This is the default.

Sort lets you sort events in terms of event priority, type, node class, name, or time.

Options — **Filters...** control the events displayed. Pull down **Options>Filters** to edit filters. Pull down the priority status or device class or enter a node name, or a time span. These parameters control the events that are displayed by **View**.

Find... lets you specify a string to be searched for in the Notepad.

Copy selected to Clipboard lets you copy all selected events to the Clipboard, so you can paste the text into another application (e.g., a word processor).

Go to Node lets you go directly to a specific node in the table without having to scroll through the entire Event Browser.

Acknowledge — Lets you acknowledge many events at once. **Selected** acknowledges highlighted events. **Filtered** acknowledges filtered events or, if no filter is set, all events. **All** acknowledges all events.

5.2.6 Thresholds

You can give a threshold value to any data item. When this threshold value is exceeded, an Information event is generated. For example, an event can be generated when the number of error packets reaches a specified level. Thresholds are established in the Graphing or Logging applications. Thresholds are only valid while the graph or log is running.

Two events are always generated for any threshold: one when it is exceeded, and another one when the data value drops below the threshold. This lets you calculate the time that the threshold was exceeded and minimizes the number of event messages generated.

5.2.7 The Event Log

The Event log is a file containing records of all events over a number of sessions. The first file is named `EVENTB.000` and resides in the directory `C:\fb500\lan`. A new file, numbered sequentially, is opened after every 500 events. You can save logs to a file on the FIREBERD 300/500's hard drive or a floppy disk. Delete the Event log file when past events become irrelevant, to free up disk space.

5.3 USING THE GRAPH DATA TASK

You can graph any of the objects that make sense to graph. Each graph can plot up to seven parameters. You can run up to five graphs simultaneously. You can start up a second Graph Data task, allowing for another set of graphs. The trade-off is that the LAN Analyzer's performance is slower while multiple graphs are running.

NOTE: When more than one analyzer has been selected, clicking on the Graph Data icon displays the Select Multiple Analyzers dialog box. Select the desired analyzer(s) by clicking on the desired analyzer(s), then ckick on **OK** to display the Graph Parameters dialog box.

5.3.1 Setting Graph Parameters

To begin a graph, click on the Graph Data icon. The Graph Parameters dialog box is displayed. **MIB Browse Groups** with their objects are as shown in Figure 5-2.

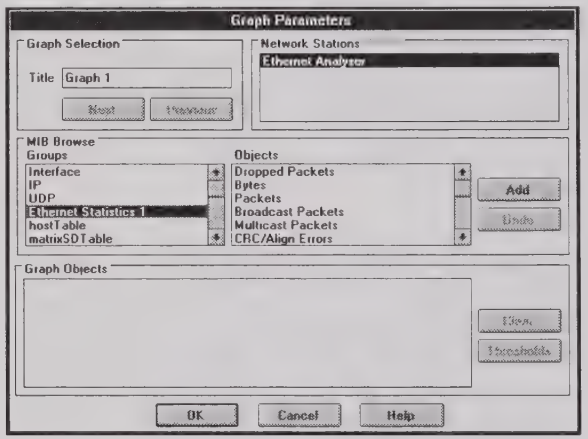


Figure 5-2
Graph Parameters Dialog Box

Network Stations Displays the station selected when you entered graphing.

To set up a graph, do the following:

1. Under **MIB Browse Groups**, highlight and click on a group for which you want to graph a parameter. For example, this could be a group or a table. A list of parameters then appears in **Objects**.

2. Under **Objects**, select the parameter(s) that you want to graph for this device. To select more than one item, hold down **<Ctrl>**, click the trackball button, and drag the cursor over each item you want to select.

3. Click on **Add** to add the selected parameter(s) to the **Graph Objects** list.

4. Set any thresholds you want by clicking **Thresholds**. When a parameter reaches a threshold value, an event is generated. All points are plotted on the graph whether they are above or below this threshold level, but setting a threshold shows more clearly when a significant level is exceeded. Rates are measured per second. Any thresholds you don't need should be left blank, to keep the graph clear and avoid generating unneeded events.

When you have finished entering graph parameters, click on **OK** to start the graph. If a graph is already running, you are asked if you want to restart it. **Clear** removes all the parameters from the **Objects** list. **Undo** cancels a change in the graph parameters or removes the most recent addition to the **Objects** list.

5.3.2 Running Multiple Graphs

After setting up one graph, select **Next**. This lets you enter parameters to be displayed on a second graph. You can run up to five graphs simultaneously. Use **Previous** to look at the parameters of an earlier graph.

5.3.3 Ethernet Graphable Variables

Click on the Graph Data icon. FIREBERD Ethernet variables are contained in the two groups called EthernetStatistics1 (RMON MIB variables) and FIREBERDStatistics1 (TTC-enterprise RMON-extension variables):

EthernetStatistics1

Dropped Packets	The total number of events in which packets were dropped due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
Bytes	The total number of octets (8 bits) of data, including those in bad packets, received on the network (excluding framing bits, but including FCS octets).
Packets	The total number of multi-byte units of data (including error packets) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address.
Multicast Packets	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC/Align Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad FCS.
Short Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Long Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were not an integral number of octets in length or that had a bad FCS, and were less than 64 octets in length (excluding framing bits, but including FCS octets).
Jabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets in length or had a bad FCS).
Collisions	The best estimate of the number of the total number of collisions on this Ethernet segment.
64 Byte Packets	The total number of packets (including error packets) received that were 64 octets in length (excluding framing bits, but including FCS octets).
65->127 Byte Packets	The total number of packets (including error packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits, but including FCS octets).
128->255 Byte Packets	The total number of packets (including error packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits, but including FCS octets).
256->511 Byte Packets	The total number of packets (including error packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits, but including FCS octets).
512->1023 Byte Packets	The total number of packets (including error packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits, but including FCS octets).
1024->1518 Byte Packets	The total number of packets (including error packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits, but including FCS octets).

FIREBERD Statistics 1

Valid Bytes	The total number of octets of data (excluding those in bad packets) received on the network (excluding framing bits, but including FCS octets).
Valid Packets	The total number of packets (excluding error packets) received on the network.
Error Packets	The total number of error packets received on the network.

Segment Load (x100%)	The best estimate of the mean physical layer network utilization on this interface (including error packets) during the last second, in hundredths of a percent.
Valid Segment Load (x100%)	The best estimate of the mean physical layer network utilization on this interface (excluding error packets) during the last second, in hundredths of a percent.
Packet Rate	The total number of packets (including error packets) received on the network in the last second.
Valid Packet Rate	The total number of packets (excluding error packets) received on the network in the last second.
Broadcast Rate	The total number of good packets received in the last second that were directed to the broadcast address.
Multicast Rate	The total number of good packets received in the last second that were directed to the multicast address. This number doesn't include packets directed to the broadcast address.
Error %	The percentage of error packets to total packets received on the network in the last second, in hundredths of a percent.
CRC/Align % (x100)	The percentage of CRC or Alignment error packets to total packets received in the last second, in hundredths of a percent. CRC/Alignment error packets are packets that have a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets inclusive, but were not an integral number of octets in length or had a bad FCS.
Short Packet % (x100)	The percentage of short packets to total packets received in the last second, in hundredths of a percent. Short packets are packets that are less than 64 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
Long Packet % (x100)	The percentage of long packets to total packets received in the last second, in hundredths of a percent. Long packets are packets that are longer than 1518 octets long (excluding framing bits, but including FCS octets) and are otherwise well formed.
Fragment % (x100)	The percentage of fragments to total packets received in the last second, in hundredths of a percent. Fragments are packets that are not an integral number of octets in length or that have a bad FCS, and are less than 64 octets in length (excluding framing bits, but including FCS octets).

Jabber % (x100)	The percentage of jabbers to total packets received in the last second, in hundredths of a percent. Jabbers are packets that are longer than 1518 octets (excluding framing bits, but including FCS octets), and are not an integral number of octets in length or have a bad FCS.
Collision Rate (x100)	The best estimate of the number of collisions in this Ethernet segment in the last second.

5.3.4 Token Ring Graphable Variables

FIREBERD 300/500 Token Ring variables are contained in the two groups called tokenRingMLStatsTable1 (RMON MIB variables) and tokenRingPStatsTable1:

tokenRingMLStatsTable1

TokenRingMLStatsDropEvents	The total number of events in which packets were dropped due to lack of resources. This number does not necessarily include the number of packets dropped; it is just the number of times this condition has been detected.
TokenRingMLStatsMacOctets	The total number of octets of data in MAC packets (excluding those in packets with FCS errors) received on the network (excluding framing bits, but including FCS octets).
TokenRingMLStatsMacPkts	The total number of MAC packets (excluding packets with errors) received.
TokenRingMLStatsRingPurgeEvents	The total number of times that the ring enters the ring purge state from normal ring state. The ring purge state that comes in response to the monitor contention or beacon state is not counted.
TokenRingMLStatsRingPurgePkts	The total number of ring purge MAC packets detected by the analyzer.
TokenRingMLStatsBeaconEvents	The total number of times that the ring enters a beaconing state (beaconFrame StreamingState, beaconBitStreamingState, or beaconSetRecovery ModeState). A change of the source address of the beacon packet does not constitute a new beacon event.
TokenRingMLStatsBeaconPkts	The total number of beacon MAC packets detected by the analyzer.

TokenRingMLStatsMonitorContentionEvents	The total number of times that the ring enters the monitor contention state from normal ring state or ring purge state. The monitor contention state that comes in response to a beacon state is not counted.
TokenRingMLStatsClaimTokenPkts	The total number of claim token MAC packets detected by the analyzer.
TokenRingMLStatsNAUNChanges	The total number of NAUN changes detected by the analyzer.
TokenRingMLStatsLineErrors	The total number of line errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsInternalErrors	The total number of adapter internal errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsBurstErrors	The total number of burst errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsACErrors	The total number of Address Copied (AC) errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsAbortErrors	The total number of abort delimiters reported in error reporting packets detected by the analyzer.
TokenRingMLStatsLostFrameErrors	The total number of lost frame errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsCongestionErrors	The total number of receive congestion errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsFrameCopiedErrors	The total number of frame copied errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsFrequencyErrors	The total number of frequency errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsTokenErrors	The total number of token errors reported in error reporting packets detected by the analyzer.
TokenRingMLStatsSoftErrorReports	The total number of soft error report frames detected by the analyzer.

TokenRingMLStatsRingPollEvents	The total number of ring poll events detected by the analyzer (i.e., the number of ring polls initiated by the active monitor that were detected).

tokenRingPStatsTable1

TokenRingPStatsDropEvents	The total number of events in which packets were dropped by the analyzer due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
TokenRingPStatsOctets	The total number of octets of data (excluding those in bad packets) received on the network (excluding framing bits, but including FCS octets) in non-MAC packets.
TokenRingPStatsPkts	The total number of non-MAC packets (excluding packets with errors) received.
TokenRingPStatsDataBroadcastPkts	The total number of good non-MAC packets received that were directed to a LLC broadcast address (0xFFFFFFFFFFFF or 0xC000FFFFFFFF).
TokenRingPStatsDataMulticastPkts	The total number of good non-MAC packets received that were directed to a local or global multicast or functional address. This number does not include packets directed to the broadcast address.
TokenRingPStatsDataPkts18to63Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 18 and 63 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts64to127Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 64 and 127 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts128to255Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 128 and 255 octets in length inclusive, excluding framing bits, but including FCS octets.

TokenRingPStatsDataPkts256to511Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 256 and 511 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts512to1023Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 512 and 1023 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts1024to2047Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 1024 and 2047 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts2048to4095Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 2048 and 4095 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts4096to8191Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 4096 and 8191 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPkts8192to18000Octets	The total number of non-MAC packets (excluding packets with errors) received that were between 8192 and 18000 octets in length inclusive, excluding framing bits, but including FCS octets.
TokenRingPStatsDataPktsGreaterThan18000Octets	The total number of non-MAC packets (excluding packets with errors) received that were greater than 18000 octets in length, excluding framing bits, but including FCS octets.

5.3.5 The Graph Display

The Graph display can show several graphs at once, as windows or icons, or a mix of the two. Figure 5-3 shows one graph window and an iconized graph.

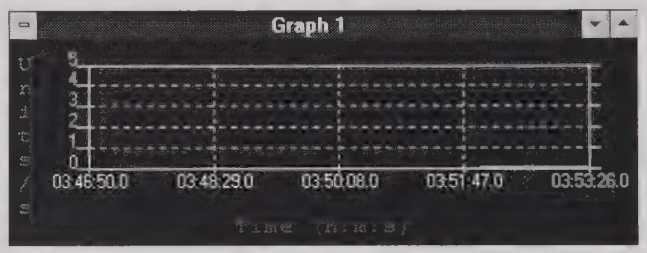


Figure 5-3
Graph Display

Features of the display for each graph are:

Data — Plots data using the information from the Graph Parameters box. Plotting begins after two polls. Data can be shown as absolute figures or a rate over time (per second). You can't plot aggregates for devices or parameters, but you can set threshold values for parameters and show these on the graph. Crossing these statistical thresholds produces an Event.

Axes — The graph is scaled automatically, although you can overrule this. Set the Y axis using **View>Y Scale**.

Key — To see what the plots represent, double-click on the **Key** icon.

NOTE: — Once data has been deleted from the displayed graph, it can't be retrieved. You must restart the graph before changing the parameters displayed or the poll rate, or setting the thresholds. You can, however, change the Y scale.

5.3.6 Graph Options

The graph options displayed at the top of the graph display are:

File

New... — Asks for parameters for a new graph. This does not destroy existing graphs: you can run up to five graphs at once.

Exit — Closes the graph application and all running graphs.

Edit

Copy to Clipboard — Copies the graph, as a bitmap, to the Windows Clipboard. From there you can copy it into a spreadsheet or other application.

View

Graph Title — The graph title is displayed in the title bar above the graph.

Rate Graph — A rate graph always shows parameters as a rate per second. This takes two values and divides the difference between them by the polling interval. Most MIB II parameters are best shown as a rate.

Absolute Graph — Plots absolute values, not rates. Use this selection to display data held as a rate in the MIB itself. For example, the LAN Analyzer has a MIB variable that measures the % load rate as a rate per second.

Show Thresholds — Displays thresholds you have set.

Y Scale — Pull right to show **Auto** and a range of values, from 5 to 500 Million and Maximum. **Auto** keeps the Y scale reasonable, but you can set one of the other values if necessary. **Auto** extends the graph as values increase, but does not reduce it again if values fall back. You can normally scale it down by selecting **Auto** again.

Configure

Graph Parameters — Sets up parameters and thresholds for display, altering them for a running graph. This has already been described. The **Graph Objects** list in the dialog box initially shows the current parameters. You can change this list using the **Add** and **Clear** buttons. You can also add or change thresholds.

Poll Rate — Controls the frequency of polling for this graph. This modifies only the poll rate used for plotting graphs, not other poll rates. Different graphs can poll at different rates. The default poll rate is 2 seconds. Changing the poll rate restarts the graph. Enter the poll rate in hours, minutes, and seconds. Then click on **OK**. You are warned that an existing graph will be restarted (plotted values will be cleared). You can abandon the change by clicking on **Cancel**.

Window

Tile — Places open windows next to each other so they don't overlap. This lets you simultaneously view all open running graphs.

Cascade — Arranges windows in an overlapping pattern so the title bar of each window is visible.

Arrange Icons — Arranges graph file icons neatly, so they don't overlap.

When you click on **OK** after making changes, you are warned that the existing graph will be restarted. This means you will lose all existing data. If you need this data, use **File>New** to create a new graph without overwriting the existing graph.

5.4 USING THE LOG DATA TASK

Logging is the process of storing parameter data over time in a file. This is in many ways similar to graphing. You can log any of the variables supported within a station's MIB. Each log can hold up to seven parameters. These can be seven parameters for one node, one parameter for seven nodes, or any other combination. You can run up to five logs simultaneously from one log application. You can go back to the LAN Analyzer's top-level menu to start a second log application, allowing for more logs.

NOTE: When more than one analyzer has been selected, clicking on the Log Data icon displays the Select Multiple Analyzers dialog box. Select the desired analyzer(s) by clicking on the desired analyzer(s), then ckick on **OK** to display the Log data box.

5.4.1 Setting Logging Parameters

To set up a log, click on the Log Data icon on the LAN Analyzer's top-level menu. The Log Data box is shown in Figure 5-4.

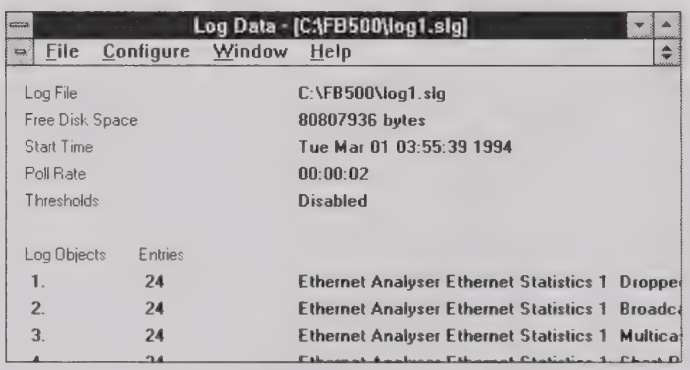

Log Data - [C:\FB500\log1.slg]
File Configure Window Help
Log File C:\FB500\log1.slg
Free Disk Space 80807936 bytes
Start Time Tue Mar 01 03:55:39 1994
Poll Rate 00:00:02
Thresholds Disabled
Log Objects Entries
1. 24 Ethernet Analyser Ethernet Statistics 1 Droppe
2. 24 Ethernet Analyser Ethernet Statistics 1 Broadc
3. 24 Ethernet Analyser Ethernet Statistics 1 Multica

Figure 5-4
Setting Log Parameters

To set up a log, do the following:

1. Enter the name of the file where the data is to be stored, or use the default name. If this will overwrite an existing file, you are warned before the file is overwritten. You can then change the name.

2. Under **MIB Browse**, select a group for which you want to log a parameter (e.g., a group or a table). If you have a Token Ring and an Ethernet analyzer, the MIB **Browse Groups** only lists the groups that are common to both types.

3. Select the parameters from the **Objects** list that you want to log for this device component. To select more than one item, hold down **<Ctrl>**, click the trackball button, and drag the trackball over each item you want to select.

4. Click on **Add** to add the selected parameters to the **Log Objects** list.

5. Set any thresholds you want by clicking **Thresholds**. An event is generated when a parameter reaches a threshold value. Events are logged whether they are above or below this value. The thresholds that you don't need should be left blank, so you only generate the events that are useful to you.

Figure 5-5 shows the Threshold Browser dialog box.

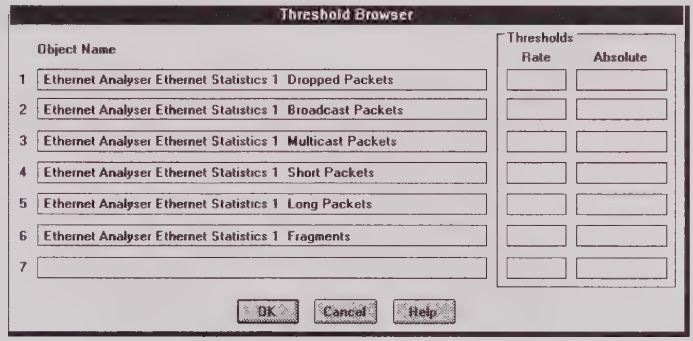


Figure 5-5
Specifying Threshold Values

When you have finished entering log parameters, click on **OK** to start the log. If a log of the same name is already running, you are asked if you want to overwrite it. Clicking on **Clear** removes objects from the **Log Objects** list. **Undo** cancels a change made to the log parameters, it removes the most recent addition to the list of Log Objects.

5.4.2 The Log Display

The Log application window shows a representation of each log you run. Logs are shown as either windows or icons, or a mix of the two. Figure 5-6 shows log1.slg (Log 1) as a window and an iconized second log (log2).

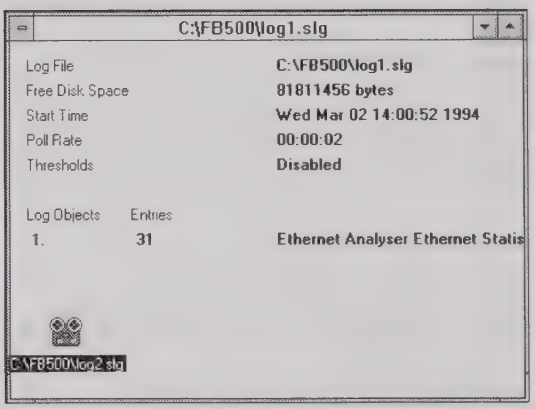


Figure 5-6
Log Application Window

NOTE: Data does not actually appear in the log display. All logged data is stored in a file, which can be read by a spreadsheet program.

5.4.3 Logging Options

The Logging options at the top of the display are:

File

New... Asks for parameters for a new log. This does not replace existing logs; you can run up to five logs at once.

Exit Closes the log application. All logs are closed and the file saved. To remove just one log, click on the control-menu box and click on **Close**.

Configure

Logging Parameters Sets up parameters and thresholds for display. This is where you start when you begin logging. The **Log Objects** list in the dialog box initially shows the current parameters. You can change parameters using **Add** and **Clear**. Also, you can add or change thresholds.

Poll Rate	Controls the frequency of polling for this log. Different logs can poll at different rates; the default poll rate is 2 seconds. Changing the poll rate restarts the log. Enter the poll rate (in hours, minutes, and seconds) and click on **OK**. You're warned that an existing log will be overwritten and you can abandon the change if you want.
Window	
Tile	Places open windows next to each other so they don't overlap. This lets you simultaneously view all open running logs.
Cascade	Arranges windows in an overlapping pattern so the title bar of each window is visible.
Arrange Icons	Arranges log file icons neatly, so they don't overlap.
Help	
Index	Displays the Log Data On-Line Help topic.
About Log Data...	Displays the software version of Log Data.

You cannot reset parameters or the poll rate without restarting the graph. When you click **OK** after making changes, you are warned that the existing file will be overwritten and the display will be restarted. This means you will lose all existing data. If you need this data, use **File>New** instead. This creates a new log without overwriting the existing log.

Closing a Log

Click on the control-menu box in the upper left corner of the Graph Data display to close a log file.

5.5 THE ADDRESS TRANSLATION TABLE

The Address Translation Table enables you to refer to stations on the network by names you assign, rather than by MAC Addresses. This table also groups the stations by MAC Address, Name, Segment, and IP Address. The LAN Analyzer performs the address translation automatically the first time you run a Task.

The Address Translation Table's icon is located at the bottom of the screen when the LAN Analyzer's main menu is displayed. Double-click on the icon to access the Address Translation Table. Figure 5-7 shows the Address Translation Table.

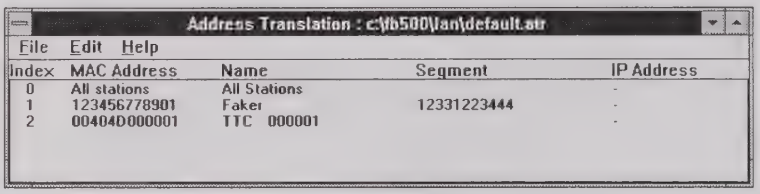

Address Translation : c:\fb500\lan\default.atr
File Edit Help
Index MAC Address Name Segment IP Address
0 All stations All Stations -
1 123456778901 Faker 12331223444 -
2 00404D000001 TTC 000001 -

Figure 5-7
Address Translation Table

The top-level menu choices in the Address Translation Table are:

File

Save Table... Saves the Address Translation Table to a file, the default directory is `C:\fb500\lan` and the default extension for filenames is `.atr`.

Load Table... Recalls and loads stored Address Translation Table files.

Merge .S01 File... Opens and allows you to use the `.atr` files you've created.

Exit Ends the session in the Address Translation Table.

Edit

Add Entry... Enables you to add an entry to the Table. Include the station's MAC Address, name, and segment (segment is optional information).

Edit Entry... Enables you to make changes to an entry to the Table. Highlight the entry you want to edit, pull down **Edit>Edit Entry...**, and change as needed.

Delete Entry Enables you to remove to an entry from the Table. Highlight the entry you want to delete, pull down **Edit>Delete Entry...**.

Sort by Arrange to view the entries according to **MAC Address**, **Name**, or **Segment**.

Define Group... A group is any stations you want to have included in the Table.

Read from probes... Displays the analyzer cards loaded on the LAN Analyzer. Highlight the appropriate analyzer card and click on **OK** to select it to be read.

Help

General Index	Provides an index to the topics in the LAN Analyzer's On-Line Help.
Address Translation	Displays context-sensitive information about the Address Translation Table.
About ATR...	Displays the software version of the Address Translation Table.

When you finish the LAN Analyzer session without saving changes to the Address Translation Table, the LAN Analyzer asks you whether you want to save changes to the Table.

5.6 TELNET

Telnet is the protocol the LAN Analyzer uses to log in to a remote host (as long as the host is running a Telnet server). Once you are logged onto the remote station, you appear to be connected locally.

Click on the Telnet icon on the LAN Analyzer's main menu to enable Telnet, and bring up the Telnet window. Figure 5-8 shows the Telnet window.

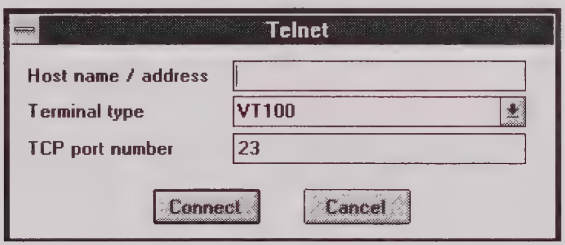


Figure 5-8
Telnet Window

The choices in this window are:

Host name / address	Enter up to 26 alphanumeric characters for the name and address of the host you want to remotely administer.
Terminal type	Three terminal types are available: Glass, ADM3A, and VT100. The VT100 type is the default, and it includes the functions used by most hosts. If the remote host does not support Telnet, this is grayed out.
TCP port number	Most devices use port 23 for Telnet, so 23 is the default setting.

Click on **Connect** to establish the Telnet connection. If the station does not support Telnet, the LAN Analyzer displays an error message.

APPENDIX A
PC/TCP SOFTWARE

A.1 INTRODUCTION

This appendix provides additional information concerning the PC/TCP software that is loaded on your LAN Analyzer. This information is intended to provide you with an overview of FIREBERD 300/500-specific information that is contained in the FTP PC/TCP manual.

The following two commands provide information on the network status. If ping did obtain a satisfactory response, use either of these commands:

- `Host` is useful if you are using a name server. It looks up the Internet address corresponding to a character string name. `Host` sends an inquiry to each name server that was specified at configuration time using the `ipconfig` command. Use host to isolate problems that cause erratic host name resolution.
- `Inet` displays a variety of network statistics.

A.2 COMMAND DESCRIPTION

You can use the programs described in the following paragraphs to test PC/TCP, to be sure it is operating correctly. You can only run these programs from DOS. You cannot use them from Windows or the Test Manager. These are: Ping, Host, and Inet.

A.2.1 Ping

`Ping` sends an echo request to another host and watches for a response using the ICMP/IP protocol. It is used primarily to isolate trouble in an internetwork environment. PC/TCP always responds to echo requests.

The following are two variations of ping.

ping [*option(s)*] hostname

or

ping -version

The variable *hostname* is either a character-string name of the destination or an Internet address in standard form. See Section A.5, Host Names and Internet Addresses for more details.

The *-version* option displays the version number and patch level of the **ping** program you are running. You should know the version and patch level of the program whenever you report problems to your local technical support.

In the example below, the LAN Analyzer sends an echo request to the host "wayward" and displays statistics about the connection.

```
ping wayward

host responding, time = 25 ms

Debugging information for interface (1, 0) Addr(6): 08 00 4e 03 1c 57 interrupts:
0 (4263 receive, 0 transmit)
packets received: 4263, transmitted: 632
receive errors: 0, unknown types: 0
        runts: 0, aligns: 0, CRC: 0, parity: 0, overflow: 0
        too big: 0, out of buffers: 0, rcv timeout: 0, rcv reset: 0
transmit errors: 0
        collisions: 0, underflows: 0, timeouts: 0, resets: 0
        lost crs: 0, heartbeat failed: 0
ARP statistics:
arps received: 860 (807 requests, 53 replies)
        bad: opcodes: 0, hardware type: 0, protocol type: 160
arps transmitted: 96 (92 requests, 4 replies)
20 packet buffers; 20 free now; minimum of 13 free
```

A.2.2 Ping Options

Valid options for **ping** are:

-d *[bytes]*	Print out header information and a dump of the incoming packet in hex. If specified, *bytes* tells the number of bytes to print out. The default is to print only the header. If the "-t" option is also selected, **ping** prints out the first input packet.
-d# *[bytes]*	Print out header information and a dump of the outgoing packet in hex. If specified, *bytes* tells the number of bytes to print out. The default is to print only the header. If the "-t" option is also selected, **ping** prints out the first input packet.
-e	Cancel IP extended security options. If any IP extended security options are configured, **ping** will insert them unless you use this option.
-i *seconds*	Ping the remote host with the IP Time to Live option set to *seconds*.
-j *dest 1... dest n*	Ping the remote host with the Loose Source Routing turned on. Each destination uses 4 bytes of option space.

-k *dest 1... dest n* Ping the remote host with the Strict Source Routing turned on. Each destination selection uses 4 bytes of option space.

-l *length* Set the number of bytes of data to *length.* The default value is 256 bytes.

-n *no_times* Ping the remote host *no_times* times, then stop.

-o Ping the remote host with the IP No-Op option set. This option has no effect on the transmission, but is sometimes used for alignment purposes. It uses 1 byte of option space.

-p *precedence* Ping the remote host with the IP precedence option set to *precedence.* This option overrides any precedence options configured with `ipconfig`. Valid precedence levels are given below.

Value	Precedence
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash override
5	CRmC/ECP
6	Internetwork control
7	Network control

-r Ping the remote host with the Record Route option turned on.

-t Go into a loop continually sending echo requests to host *hostname,* each time waiting for a response before sending the next request. To exit this loop, type the single letter "q." When in looping mode, `ping` reports all echo failures, and also maintains a summary line of trials and successes.

-v *type* Ping the remote host with the IP Type of Service option set to *type.* This option overrides any Type of Service options configured with `ipconfig`. The list below shows the valid values for *type.*

Value	Type of Service
0	Normal
1	High reliability
2	High throughput
3	High throughput, high reliability
4	Low delay
5	Low delay, high reliability
6	Low delay, high throughput
7	Low delay, high throughput High reliability

-x option Ping the remote host with the IP Timestamp option turned on. The default is not to record timestamps. Each option takes up 8 bytes of option space. The valid *options* are:

1	Fill in the host address with each timestamp recorded.
3 *dest 1...dest n*	Fill in only hosts at the designated addresses with timestamps.

-z Quiet mode. **ping** will only report success or failure, not full statistics.

NOTE: Options "-e," "-j," "-k," "-o," "-r," and "-x" add IP options to the packet header. Option space is limited to a total of 40 bytes. Some options have a fixed length, others may be any length up to the 40-byte limit. You may combine options, and the space **ping** allots to a variable length option depends on what else is selected. Variable length options take up 3 bytes of header space as well as whatever is used by the data. If the selected combination total is more than 40 bytes, **ping** prints out an error message and exits.

Ping reports success with a message such as "Host responding", and an array of statistics about the connection (in the same format as **inet debug**. This information is most useful when you run **ping** in a loop.

A.2.3 Error Messages from Ping

Ping reports failure with the message **Ping failed** and one of the following error messages:

The initial echo request packet could not be sent.
The Analyzer received a hardware or routing error to the ICMP echo request.

Out of resources (memory/connections).
Out of resources, usually due to a lack of packet buffers. The output from the **inet debug** command may indicate excessive broadcast packets on the net.

Host unreachable.
The address is on the local net/subnet, but the hardware returned transmit error, or the foreign host did not respond to the ARP request.

Network unreachable.
The address is not on the local net/subnet, and either no gateway is set or the gateway did not respond to the ARP request.

Bad response from server.
The Analyzer received an ICMP Echo Reply with the correct sequence, but bad data or checksum.

Timeout.

No ICMP Echo Reply with the correct sequence number was received from the remote host within the 6-second timeout period. This message indicates that the Echo Request was sent without error, and that the ARP succeeded for the host, or for the gateway, if the host isn't on the local net/subnet.

A.2.4 Using Ping To Isolate Network Trouble

When a host fails to respond, it may mean either that host is down or that some network or gateway in the path from the user to the host is down. (It could also mean that the host does not implement the ICMP/IP echo request protocol.) Further **ping** experiments can usually determine which is the problem.

A successful **ping** directed to another host on the same network as the original host usually means that the original host is down or not listening to the network. Failure to get echoes from any host on that network means that the trouble is along the path somewhere. A **ping** directed to the gateway into the network in question is the next step. You can continue to work back from the destination toward the originator until you find the point where communication breaks down.

The echo request sent by the **ping** command is dispatched using a low-level protocol that does not try to guarantee delivery. As a result, there is a possibility that any one echo request may be accidentally lost for a reason such as temporary overload in some gateway. Therefore, you cannot be sure that a particular network or gateway has failed unless a series of **ping** experiments consistently succeeds in getting to that point and consistently fails to get beyond it.

A.2.5 Host

Host looks up the Internet address that corresponds to a character string name, using all available name protocols. **Host** first tries to look up the name in a host table, if there is one. If this fails, **host** then tries using the UDP domain name protocol.

Type the command using one of the following formats.

host *[method] [-s name-server] <host 1>...<host n>*

or

host *-version*

The *-version* option displays the version number and patch level of the host program you are running. You should know the version and patch level of the program whenever you report problems to your local technical support.

Example: `host -t wayward`

This produces the following:

```
by host-table, wayward: 89.0.2.71, cname is wayward.wayward.co.uk
```

In the example, **host** asks the host table (previously configured with ipconfig) for the Internet address of the host "wayward," then displays the response it receives.

The parameters for **host** are:

method — The name resolution method to use to resolve the host name. The default resolution method is **a**. The options available are as follows:

- -a Try all name resolution methods.
- -d Try all of the configured domain name servers.
- -t Try the configured host table.

-s name-server — An optional argument that identifies a name server to be invoked to resolve the name. The *name-server* may be either a character string name, which is resolved using the configured name servers, or an Internet address in standard form.

host 1...host n — The character string host name(s) to be resolved.

Host Names and Internet Addresses provide additional information to aid the resolution of host names. The **host** command is useful primarily for trouble isolation when you suspect that name tables may be inconsistent or incorrect.

A.2.6 Inet

inet displays a range of network statistics. The **inet** command can be in either of the following formats.

inet *option*

or

inet *-version*

The *-version* option displays the version number and patch level (if any) of the **inet** program you are running. Patch levels are upgrades to the program that are released between versions. You should know the version and patch level whenever you report problems to your local technical support.

Example: **inet** arp

This produces the following:

```
FTP Software PC/TCP inet Version 3.0
Copyright (c) 1986-1994 by FTP Software, Inc.  All rights reserved.

ARP cache:
  128.127.2.132:       0000c0752b1c       expires: 856 sec.
  128.127.2.102:       0800200227e0       expires: 852 sec.
  128.127.2.101:       08002b06227d       expires: 847 sec.
  128.127.2.100:       08002b03e7c0       expires: 843 sec.
  128.127.2.135:       0000c08b9710       expired
```

A.2.7 Inet Options

All of the following options can be given on the same command line. However, if you use the *unload* option, you must make it the last option on the command line.

arp

Display the current contents of PC/TCP's ARP cache. The ARP cache contains entries for each object on the network that has either sent PC/TCP an ARP request or replied to an ARP request from PC/TCP. The cache can hold up to 40 entries.

An ARP cache entry consists of the object's Internet address, physical address, and the number of seconds remaining before the entry expires (is no longer valid).

An entry expires 15 minutes after it was last used. An expired entry, marked `expired`, may remain in the cache table.

config

Display the following information:

- The date and time PC/TCP began running.
- The number of TCP, UDP, and IP connections open or listening.
- The number of global and local descriptives active.
- The Internet broadcast address on PC/TCP.

If the broadcast address is not correct, you can change it only by unloading PC/TCP and reloading it with the correct address.

IMPORTANT: Do not change the broadcast address unless you cannot connect to other hosts without changing it. If you do change the broadcast address, TTC cannot guarantee that your network will perform properly.

debug Display the following information:

- The MAC (physical address) of the interface.
- The number of packets received and transmitted.
- The number of receive errors.
- The number of transmit errors.
- ARP statistics.
- The number of free packet buffers.

help Display information about the **inet** program and its arguments.

route Display the current contents of PC/TCP's routing cache. The routing cache contains the information learned through ICMP host redirect packets. The routing cache holds 16 entries.

stats Display network interface statistics. These include:

- The name of the interface.
- The IP address of the interface.
- The subnet mask.
- The total number of packets sent out and received on this interface.
- errs out.

  This is the sum of:
  (number of times hardware driver refused to send a packet) + (number of times a packet couldn't be obtained for loopback) + (number of times routing failed for packets, in other words, there was an ARP timeout or no gateway).

  See the hardware driver's error counters (if available) for more detail. Use **inet debug**.

- errs in.

  The number of packets that could not be demuxed, for one of these reasons:

  packet was too short (between 14 and 60 bytes).

  packet was not of a type the demux Task recognized, but was not broadcast. That is, the type was neither IP, ARP, nor IP-ARP, nor IP Trailer.

unload Unloads the PC/TCP kernel from memory. After using the unload argument, you can no longer use any of the other PC/TCP programs until you reload the PC/TCP kernel into memory. You can use unload to free memory for another application, or to disable network use. If you have sessions open when you issue the inet unload command, you are prompted to confirm that you really want to unload the kernel. This feature keeps you from inadvertently unloading the kernel from under some network program. If you are going to be loading and unloading the PC/TCP kernel frequently, you should load it last. If you unload the PC/TCP kernel after loading another terminate and stay resident program into program memory, you cannot reuse the memory taken up by PC/TCP.

-? Displays and explains the usage of the command line.

version Display the version number of PC/TCP in use. This does not display the patch level. To see this, you should use the **inet** *-version* command.

A.3 TROUBLESHOOTING

Problems can arise in TCP/IP networking, especially from slightly incompatible implementations or obscure hardware conditions. The following paragraphs document some of the most common error messages and problems seen, and suggests some solutions. If you still can't solve the problem, contact TTC's Applications Engineering at (800) 638-2049 or (301) 353-1550 for help.

A.3.1 Error Messages

NOTE: Error messages generated while using **ping** are listed under Section A.2.1, Ping.

This PC's internet address is not set.
You must set the Internet address in the PCTCP.INI file before you can use any PC/TCP programs.

PC/TCP resident module is not loaded; aborting program...
You must load PC/TCP by using **netstart** if you want to run PC/TCP from DOS.

Hostname Unknown.
The name was not found in the local host table (if configured) or by any of the configured domain name or old-style name servers. If the numeric form of the hostname works, then the address is not in the host table or name servers.

Name servers not responding.
Any name servers you have configured are not responding. This makes translation impossible until a name server is available. You should either set the **ipconfig** *hosttable* option or use the numeric form of the name until a name server becomes available.

A.3.2 Problems

The list below shows some of the problems you are most likely to encounter with PC/TCP, and suggests possible causes. You are unlikely to encounter most of these problems when routinely using the LAN Analyzer. They are most likely to occur when you are testing PC/TCP after you first install it.

A.3.3 Responses From The Wrong Host

- If you are using an Internet address, is the address correct for the host you are trying to reach?

  If you have mis-typed the address, you may get responses from the wrong host.

A.3.4 No Response

- If you are using an Internet address, is the address correct for the host you are trying to reach?

  If you have mis-typed the address, you may get no response.

- Is the other host up and running?

- Can you **ping** your management station from the remote host?

  Try running the **ping** program from the remote host to see if you can get an answer from your management station. If you can get an answer in one direction but not the other, check the configuration on the two hosts.

- Is the interface card properly seated? Are the cable connections solid? Are there any breaks in the cable?

- Does the interface pass the manufacturer's diagnostics? Refer to the manual that came with your Ethernet or Token Ring card.

  If all of these tests fail, contact TTC's Applications Engineering at (800) 638-2049 or (301) 353-1550.

A.3.5 Responses From Local Hosts, But Not From Another Network

- Is the gateway or network link up and running?

  If you can get to another host on the local network, but not to a host on another network, there may be problems with the gateway or network link between the two networks. If **ping** can't get an answer from the link, you have probably not configured the gateway correctly, or the link may be down. Check the router and subnet mask entries in the PCTCP.INI file.

A.4 TECHNICAL NOTES

This section describes technical details about the LAN Analyzer Module defaults and the implementation of PC/TCP. This involves interactions between PC/TCP and the LAN Analyzer module, PC/TCP and other TCP/IP implementations (especially BSD 4.2 UNIX), and some hardware considerations.

A.4.1 Ethernet Analyzer Module Defaults

The Ethernet module settings are set in software in the file `C:\fb500\lan\analyzer.ini`. This file contains the following defaults:

```
Hardware Interrupt=5
Software Interrupt=0x60
IO Address=0x300
SRAM Address=0xD0000
NVM File=C:\fb500\lan\analem1.nvm
POT File=C:\fb500\lan\S44_8m.dld
Image File=C:\fb500\lan\analem.ebi
```

These defaults, and a description of each, are listed below.

Default:	Description:
Hardware Interrupt	The Hardware Interrupt used by the module.
Software Interrupt	The Software Interrupt used by the module.
IO Address	The IO Address in the module.
SRAM Address	Memory Base Address (RAM).
NVM File	The Non-volatile memory (NOVRAM) for the module.
POT File	Power-On Test code file, this is the first thing that is executed during initialization, and runs tests of the module's functions.
Image File	The LAN Analyzer module software itself.

The first valid analyzer card entry should start with [Analyzer Card 1], the next entry should be [Analyzer Card 2], and so on.

A.4.2 Token Ring Analyzer Module Defaults

The Token Ring module settings are set in software in the file `C:\fb500\lan\analyzer.ini`. This file contains the following defaults:

```
Hardware Interrupt=10
Software Interrupt=0x66
IO Address=0x310
SRAM Address=0xD4000
NVM File=C:\fb500\lan\analtm1.nvm
POT File=C:\fb500\lan\S45_8m.dld
Image File=C:\fb500\lan\analtm.ebi
MAC File=C:\fb500\lan\eagle.caf
```

These defaults, and a description of each, are listed below.

Default:	Description:
Hardware Interrupt	The Hardware Interrupt used by the module.
Software Interrupt	The Software Interrupt used by the module.
IO Address	The IO Address in the module.
SRAM Address	Memory Base Address (RAM).
NVM File	The Non-volatile memory (NOVRAM) for the module.
POT File	Power-On Test code file, this is the first thing that is executed during initialization, and runs tests of the module's functions.
Image File	The LAN Analyzer module software itself.
MAC File	The file that contains the MAC Addressing.

The first valid analyzer card entry should start with [Analyzer Card 1], the next entry should be [Analyzer Card 2], and so on.

A.4.3 PC/TCP Packet Driver Buffers

The packet driver values for PC/TCP are set in the file `C:\fb500\lan\netstart.bat`. The LAN Analyzer sets the following values:

```
-p 20 -u 20 -t 8
```

IMPORTANT: TTC recommends that you never set the buffer values below these settings.

A.4.4 PC/TCP Interaction with the LAN Analyzer Module

PC/TCP in the FIREBERD 300/500 uses the installed LAN Analyzer module as its access to the network. The PC/TCP packet driver interfaces directly to the LAN Analyzer module software to send and receive packets over the network. Essentially PC/TCP and the LAN Analyzer module share the LAN Analyzer's network interface as a common access point to the network. They share the same MAC Address, but have unique IP Addresses. The PC/TCP IP Address and the LAN Analyzer module IP Address are shown in Section 2.2.4, Configuring PC/TCP.

A.4.5 PC/TCP Protocols

The PC/TCP programs all use the ARPAnet standard end-to-end Internet Protocol (IP) and can be used to communicate with any other host that also uses that protocol. Individual commands use higher-level ARPAnet standard protocols from the IP family, as appropriate:

- TCP — for reliable byte stream transmission.
- UDP — for a datagram service.
- ICMP — for control messages.
- Name lookup service protocol

In addition to the protocols mentioned above, PC/TCP network programs use network services commonly found in IP Ethernet network environments. These services may include:

- Name-to-host-address translation service.
- IP gateways to other IP networks.

A.4.6 IP

The IP layer does not fragment packets, but it can re-assemble received fragments. PC/TCP supports Type of Service options in the IP header. Checking of the Type of Service options occurs in the TCP layer.

If PC/TCP receives a packet which is not for an active IP protocol or TCP or UDP socket, it generates a **`destination unreachable`** error, unless the packet was a broadcast. If the packet was a network level broadcast, PC/TCP treats it as an Internet broadcast packet.

PC/TCP routes packets according to RFC 950. You specify the network address and the number of subnet bits with the **`ifconfig`** command. PC/TCP uses this mask to separate the net/subnet portion of the address from the host portion. It determines that two machines are on the same physical network if the net/subnet parts of their addresses are the same. If PC/TCP tries to send to a machine which is not on the same physical network, it routes the packet through the default gateway, specified with **`ipconfig`**. If PC/TCP receives an ICMP redirect from the gateway, it records the redirect in internal routing tables, which it scans before using the default gateway.

For more information about the net/subnet parts of a network address, refer to Section A.5.4, Internet Addresses and Subnets.

A.4.7 UDP

PC/TCP has a complete UDP implementation, including checksums. BSD 4.2 UNIX UDP had a number of problems that have been fixed in the BSD 4.3 release. Among other things, checksums were computed incorrectly, so some nodes would not accept packets from BSD 4.2 machines.

A.4.8 TCP

The TCP is a multiple connection implementation based on the IP standard. In PC/TCP, the MAXSEGSIZE options are implemented, so PC/TCP negotiates the MAXSEGSIZE with the remote host. PC/TCP also supports 4BSD UNIX keep alive packets.

A.5 HOST NAMES AND INTERNET ADDRESSES

This section briefly describes the syntax of host names and Internet addresses, and the method by which host names are resolved.

When PC/TCP accepts a hostname argument, it may be either an Internet address or a host name. All Internet addresses are 32 bits long, and are interpreted as a network number, followed by an optional subnet number, followed by a host number. Host names are converted into Internet addresses by a name resolution algorithm.

internet address An Internet address consists of four decimal integers separated by periods, for example:

```
18.9.0.87
```

Each integer represents one byte of a 32-bit standard Internet address. When the user supplies an Internet address, PC/TCP uses it as is, requiring nothing else for name resolution.

hostname When PC/TCP encounters a string that does not appear to be an Internet address, it interprets the string as a host name and it attempts to resolve the name by searching a local host table and/or by consulting one or more name servers via the network. The pathname of the host table, if it is used, and the addresses of the name servers, must be configured with the **`ipconfig`** command in the `PCTCP.INI` file.

The algorithm described below is used to convert a host name into an address for internal use by the program.

A.5.1 Hostname Resolution

PC/TCP has a simple domain name resolver, which all executable programs use as well as a local host table. The domain name resolver depends on the name server supporting recursion. Recent versions of the bind UNIX domain name system have supported recursion.

PC/TCP uses the following algorithm when trying to resolve hostname **`fred`**:

If **`fred`** is either a decimal or octal numeric address
then parse **`fred`** and return the result.

If the host-table parameter is set in PCTCP.INI
then try to look up **`fred`** in the host table
    if it is found, then return the result.

If **`fred`** is a fully qualified domain name, then attempt a domain name resolution of **`fred`**
    if the domain name resolution fails
    then try an old style name resolution of **`fred`**
        if this resolution fails, then return an error.

If **`fred`** is not a fully qualified domain name,
then attempt a domain name resolution of **`fred.my_domain`**
    (where **`my_domain`** is the default domain specified
    in the [pctcp general] section of the PCTCP.INI file
        if that name resolution fails
        then try **`fred.arpa`**
            if that fails, then return an error.

You configure domain name servers in the [pctcp general] section of the `PCTCP.INI` file.

NOTE: If different name servers give different responses to the same inquiry, the user may see erratic results depending on which name servers are up and which respond more quickly. If you suspect that name servers are not responding or are not in agreement, the command **host** may help isolate the problem.

A.5.2 Host Table Considerations

Many TCP/IP networks are a single Ethernet cable, with only a few hosts. In this case, host tables are an economical and simple way to perform hostname to address translations. However, in larger networks (such as the DARPA Internet), there are drawbacks in using host tables, and the use of name servers is preferable. Many of these drawbacks will also affect smaller networks.

Possible problems are:

updating host tables — Unless an installation has procedures to update host tables regularly, machines will easily get out of sync and different machines will hold different addresses for certain hosts. Also, it is impossible to make immediate changes to all the host tables on the networks. When name servers are used, a single host table must be changed and then all hosts on the network will see that change from then on.

host table size — The search of the host table is linear, one line at a time, from the beginning. If the host table (for example, the standard NIC host table) is long, the lookup may take a long time.

A.5.3 Host Table Format

The host table format is the same as that of the BSD 4.2 and 4.3 UNIX operating systems.

The table is an ASCII text file. Each line is an entry. An entry consists of one numeric address and one or more names associated with that address. The address and names are separated by tabs or spaces. Comments can appear anywhere in the table. They begin with a **#** character and end at the end of the line they start on.

The first item in an entry is the Internet address. The second item contains the host name or names, beginning with the long (complete) host name. The complete name should include the domain and subdomain names, if used. Any names listed after this are separated by spaces. These can be nicknames for the host. A host may have up to 20 names, but they must all fit into 100 characters, not counting blanks, comments and the IP address.

NOTE: Host names are case-insensitive. You may enter the names in uppercase or lowercase characters.

This is an example of a small PC/TCP host table:

```
#
#                    (#)hosts              1.4            11/3/88
# Host Database
#
127.0.0.1            localhost
19.0.0.3             mole                  #
19.0.2.71            goblin bl             #Bleasdale
19.0.3.8             m24-8                 #PC
19.0.3.9             m24-9                 #PC
19.0.4.6             mvaxl                 #
19.0.32.32           vulture vult vax      #
19.0.32.1            goblinport gprt       #
19.0.32.0x9A         printserve            #Printer Server
```

A.5.4 Internet Addresses and Subnets

The NIC has provided five classes of Internet address, labeled A to E, to deal with different sizes of installation. Class A-C addresses are divided into a network portion and a local address portion. The number of bytes allocated to each portion is different for each class.

Class A addresses use the first byte to specify the class and the network address, and use the remaining three bytes for the local address. This allows 128 class A network numbers, each supporting over 16 million hosts.

Class B addresses use the first two bytes to specify the class and the network address, and use the remaining two bytes for the local address. This allows 16,864 class B network numbers, each supporting over 64,000 hosts.

Class C addresses use the first three bytes to specify the class and the network address, and use the remaining byte for the local address. This allows just over 2 million class C network numbers, each supporting 255 hosts.

The NIC does not assign Class D addresses, which are used for IP multicasting. The NIC is reserving Class E addresses for future use.

A.5.5 Subnets

It is possible to divide a class A, B, or C network into smaller subnets. These normally follow administrative divisions (such as departments), physical medium (such as Ethernet), or location.

If you use subnets, the local address is divided into a part for the subnet number and a part for the host number. The number of bits you use for each of these will depend on the number of subnets, and the number of hosts on each one.

For example, if you have a class B network number, then there are 16 bits (2 bytes) for the network address. If you use 4 bits for subnet numbers and 12 bits for host numbers, this will allow you to have 16 subnets, each with up to 4096 hosts.

INDEX

Symbols

.txt 4-64

A

AC 4-47, 4-52, 5-11
Acknowledge 5-1, 5-2
Acknowledge an event 5-1
Acknowledged events 5-2
Acknowledgment No 4-32
Add the analyzer card 3-2
Address translation table 5-21
  menu choices 5-20
ADMIN program 2-9, 2-10, 2-12
  Help command 2-10
  quit out of the ADMIN session 2-12
  reboot 2-11
  set the media type 2-10
  Token Ring speed 2-11
Alarm 4-12
Alarms 1-4
  Falling Alarm 1-2
  when a specific event occurs 1-4
  canceled 4-12
  Ethernet 4-17
  generated 4-12
  maximum 4-17
Alarms View 4-13
All protocols 4-65
Alter an existing alarm 4-15
AppleTalk 4-42
Apply box 3-5
ARP cache A-7
AUTOEXEC.BAT file 2-3

B

Banyan Vines 4-42
Beacon Frames 4-62
Begin capturing packets 4-38
Begin packet capture 4-39
Bit errors 4-51
Bit level edit 4-50
Broadcast address A-7
Buckets requested 4-44

C

Capture 1-5
  buffer 4-23
  Capture buffer control 4-38
  Token Ring packet 4-26
  Setup window 4-24
Class A A-17
Class B A-17
Class C A-17
Class D A-17
Class E A-17
Classes A-17
Clear 4-51
Clipboard 5-4
Close a log file 5-19
Close down 3-7
Colored bars 4-67
Commands
  Host A-1
  Inet A-1
  inet A-6
  Ping A-1

CONFIG.SYS 2-1
Config>Delete Config File 4-39
Config>Load from File 4-39
Configuration box 3-4
Configure Probe 4-38
Configure the alarm 4-15
Connecting to a network
  Token Ring 2-14
  10BaseT Unshielded Twisted Pair 2-14

D

Datagram length 4-28
DEC 4-42
Decodes 4-23
Default gateway A-14
Default resolution method A-6
Default router 2-6
Defaults A-11
  Ethernet module A-11
  Token Ring module A-12
Delete an existing line 4-34
Describe Analyzer box 3-2
Description 4-44, 4-60, 4-65
Destination 4-50
Destination Address 4-30
Destination and Source Fields 4-33, 4-50
Display as 4-44, 4-60, 4-65
Displaying and printing information 1-6
Displaying captured packets 4-38
Displaying the packets 4-40
Domain name server 2-8
Domain name servers A-16

E

echo request A-1, A-5
Edit Template 4-53
EISA 2-14
  add and remove boards 2-15
  EISA configuration utility 2-15
  update the EISA 2-15
Error 1-5
Error messages A-9
Error packets 4-3
Ethernet
  cumulative variables 4-45
  percentage variables 4-10
  rate variables 4-9
Ethernet media type 3-4
Ethernet packet 4-3
Ethernet variables 4-6
EthernetStatistics1 5-7
Event 5-5
Event Browser 1-2, 4-20, 5-3
  acknowledge 5-4
  File 5-4
  Options 5-4
  View 5-4
Event icon 5-1
Event log 4-12, 5-1
Event Types 5-2
  Graphing/Logging 5-2
  MIB Traps 5-2
Events 1-7, 5-1
  record of events 1-2
  log 1-4
Existing Alarms window 4-14
Exit 3-7
Exiting the LAN Analyzer 3-1
Expired entry A-7

F

Falling Alarm 4-15
FCS 4-6, 5-7
File>New 5-15, 5-19
File>Save As 4-67

File>Save As 4-39, 4-67
Filter 4-23, 4-25, 5-3
FIREBERD
  Tasks 1-4
FIREBERD 300/500
  graphing and logging features 1-7
Flag/Frag 4-29
Flag 4-29, 4-32
Fragment offset 4-29

G

Generate packets 4-49
Graph
  Config 5-15
  Edit 5-15
  File 5-14
  View 5-15
Objects 5-15
Graph Data 1-7

H

Hex field 4-49
Host A-5
Host Names A-6, A-16
Host Statistics 4-1
  list of counts 4-3
Host stats 1-4, 4-16
Host table A-5, A-16
Hysteresis 4-16

I

Subnet mask 2-7, 2-8
IBM 4-42
Identification 4-28
Incoming traffic 4-22
Information event 5-5
Installation procedure 2-2
Installing the LAN Software 2-2
Internet address A-15
Internet Addresses A-6
IP A-14
  IP Addresses 3-4
IP address 3-3
IP address resolution 2-8
IP layer A-14
IP Source 4-30
ISO 4-42

K

Key icon 4-67

L

LAN software 2-2
Length options 4-49
LLC broadcast address 5-12
LLC Fields 4-27, 4-53
Load captured packet number 4-49
Load from file 4-24
Load from probe 4-24
Load view 4-39
local address A-17
Local Area Network Analyzer Module 1-1
Log application window 5-18
Log Data 1-7
Log tables 4-12
Logging 5-16
  Config 5-18
  File 5-18
Logging options 5-18

M

MAC address 3-3
MAC fields 4-27, 4-52
Matrix statistics task 4-20
Matrix statistics view display 4-21
Matrix stats 1-4

N

Name box 3-3
Name resolution A-6
Name server 2-6
NetWare 4-42
Network interface statistics A-8
New alarms 4-15
Non-volatile memory 2-12
Not decoded 4-39
Number of buckets 4-44

O

Octet 4-3, 4-6, 5-7
Offset 4-32
Open file name 4-41
Option space A-4
Order by 4-60, 4-65
Overwritten 4-63

P

Packet 4-6
Packet Buffer 4-49
Packet driver values A-13
Packet Tests 4-58
Patch level A-5
Path 4-34
PC/TCP
  configuration file 2-8
  initialization file 2-6
  PC/TCP serial number 2-3
  software 2-3, A-1
pctcp addresses 2-8
pctcp kernel 2-7
Per-station alarms 4-16
Ping error messages A-4
Poll rate 5-15
Printing captured packets 4-68
Problems A-10
Product ID 4-53
Protocol 1-4, 4-42, 4-64
  choices 4-29
  decodes 1-1
  statistics 4-64
  stats 1-6
Protocols 1-2, 4-42, 4-65

R

Rates 5-6
Read 3-3
Ring Speed 3-4
Ring Stats 1-5
Rising alarm 4-15
Route Designators 4-52
router 2-7
Routing 4-27, 4-52
Routing cache A-8
Run Media Test 4-58

S

Sample interval 4-44
Save 1-3
  save captured packets to a file 1-5
  save error events to a file 1-5
  changes 3-7
Saving Capture Configurations 4-39
Saving specific events 1-2
Scroll bar 4-66
Search string 5-3
Segment histories 4-44
Segment history 1-5
Segment history statistics 4-45
Segment statistics view setup 4-6
Segment stats 1-4
Segment-wide alarms 4-16
Select Stations window 4-58
Session 3-7
Set up a filter 4-25
Setup a new display 4-67
Slice size 4-39
SNAP 4-28, 4-53
SNMP trap 5-1
Soft Error Frames 4-62
Source 4-50
Source Address 4-30
Start the selected tests 4-59
Starting the LAN Analyzer 3-1
Stations 4-58
Statistical data 1-2
  graphing and logging 1-2
statistics totals 4-21
Statistics View Setup 4-64
Stop Capture 4-35
Stop Capture manually 4-38
Subnet mask 2-7, 2-8
Subnet number A-17
Subnets A-17

T

Tasks 1-1, 1-3, 4-1
TCP filter template 4-53
TCP Source Port choices 4-30
TCP/IP 4-42
Telnet 1-7, 5-21
Template 4-25
  traffic generation 4-50
  choices 4-26
Test Application 1-5, 4-57
Test Manager 3-1, 3-7
Test Timeout 4-57
Time to Live 4-29
Token Ring
  percentage variables 4-11
  rate variables 4-10
Token Ring variables 4-6
tokenRingMLStatsTable1 5-10
tokenRingPStatsTable1 5-10, 5-12
top-level menus 1-2, 1-3
Traffic Generation 1-5
Traffic received 4-21
Traffic transmitted 4-21
Triggers 4-23
Tx-forward 4-58
Type 4-53
Type Field 4-51
Type of Service 4-28

U

UDP A-14
UDP domain name protocol A-5
Update every 4-60, 4-65
Updated
view 4-54
Upload size 4-41
Urgent pointer 4-33

V

Variables 4-67
Version number A-5
View title 4-41
View>Edit View 4-67
View>Freeze View 4-63
View>New 4-67
View>New View 4-40, 4-63
View>Show Info Messages 5-4
Views 4-57

W

Wildcard 4-33, 4-50
Window 4-32

X

Xerox 4-42
Xerox Echo 4-58

Telecommunications
Techniques
Corporation

Telecommunications Techniques Corporation
20400 Observation Drive, Germantown, Maryland 20876
Tel. (800) 638-2049 • (301) 353-1550 (MD) • FAX (301) 353-9216
WWW Address: http://www.ttc.com